CISSP® Common Body of Knowledge Review:

Legal, Regulations, Compliance & Investigations Domain

Version: 5.9.2

CISSP Common Body of Knowledge Review by Alfred Ouyang is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Learning Objective

Legal, Regulations, Compliance and Investigations Domain

The Legal, Regulations, Investigations and Compliance domain addresses ethical behavior and compliance with regulatory frameworks. It includes the investigative measures and techniques that can be used to determine if a crime has been committed and methods used to gather evidence (e.g., forensics). A computer crime is any illegal action where the data on a computer is assessed without permission. This includes unauthorized access or alteration of data, or unlawful use of computers and services. This domain also includes understanding the computer incident forensic response capability to identify the Advanced Persistent Threat (APT) that many organizations face today.

Reference: *CISSP CIB*, January 2012 (Rev. 5)

(cc) BY-NC-SA

Topics

Legal, Regulations, Compliance and Investigations Domain

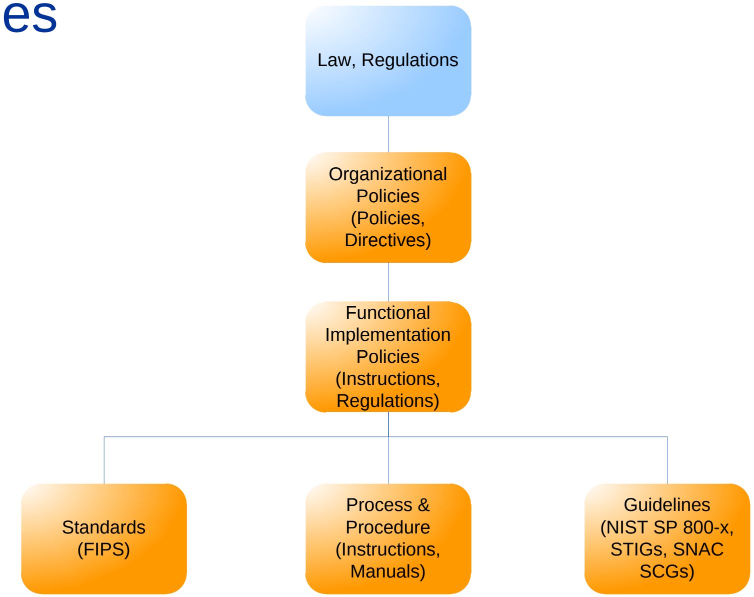
- ➡ Laws & Regulatory Compliance
- Investigations & Digital Forensics
- Ethics

(cc) BY-NC-SA

Concept

Laws & Regulations– Information Security Requirements

- Laws and regulations are the source of directive requirements (e.g. organizational policies)
- Directive requirements interpret the laws for:
  - Management to institute policy and procedure to keep the organization and its employees from violating the law.
  - Security engineering and design to keep the organization and its employees from violating the law.


Law, Regulations
Organizational Policies (Policies, Directives)
Functional Implementation Policies (Instructions, Regulations)
Standards (FIPS)
Process & Procedure (Instructions, Manuals)
Guidelines (NIST SP 800-x, STIGs, SNAC SCGs)

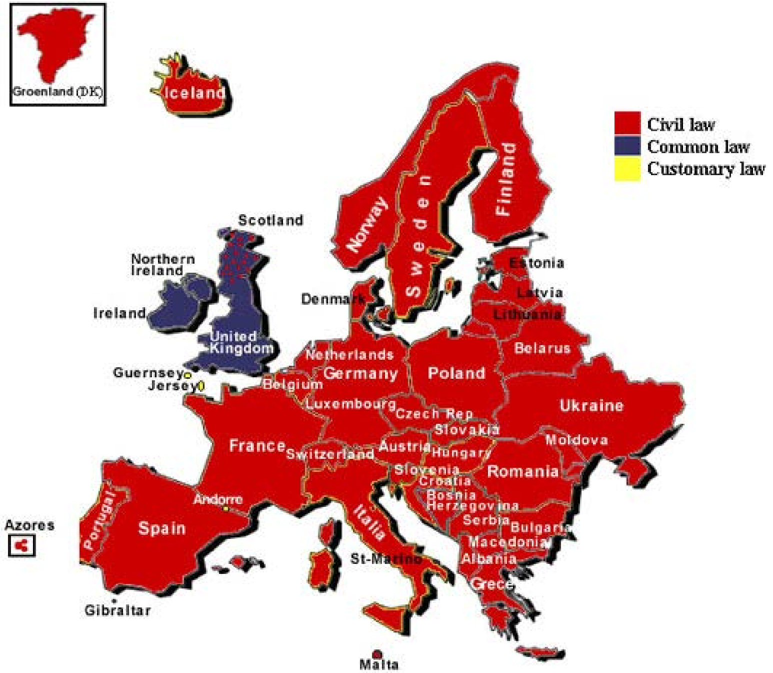
(cc) BY-NC-SA

Categories of Law ...(1/4)

- Civil law: Rule-based, not based on precedence. (ex. United States Code (U.S.C.))
  - Codification: Written rules. (e.g., Roman Law, Napoleonic Code of France, French Civil Code of 1804.)
  - Administrative law: Regulations that sets the standards of performance and conduct . (e.g. Banking regulations, SEC regulations, Insurance, FAR, EAR, ITAR.)

Belize
Guatemala
Honduras
El Salvador
Nicaragua
Costa Rica
Panama
🟥 Civil law
🟦 Common law

Aruba
Netherlands Antilles
Trinidad and Tobago
Venezuela
Guyana
Suriname
French Guyana
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Uruguay
Argentina
Chile
🟥 Civil Law
🟦 Common Law
Falkland

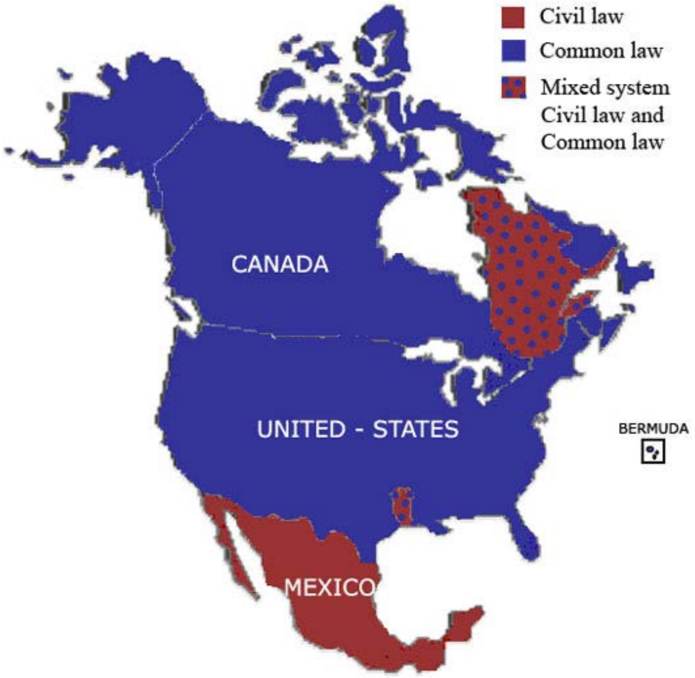


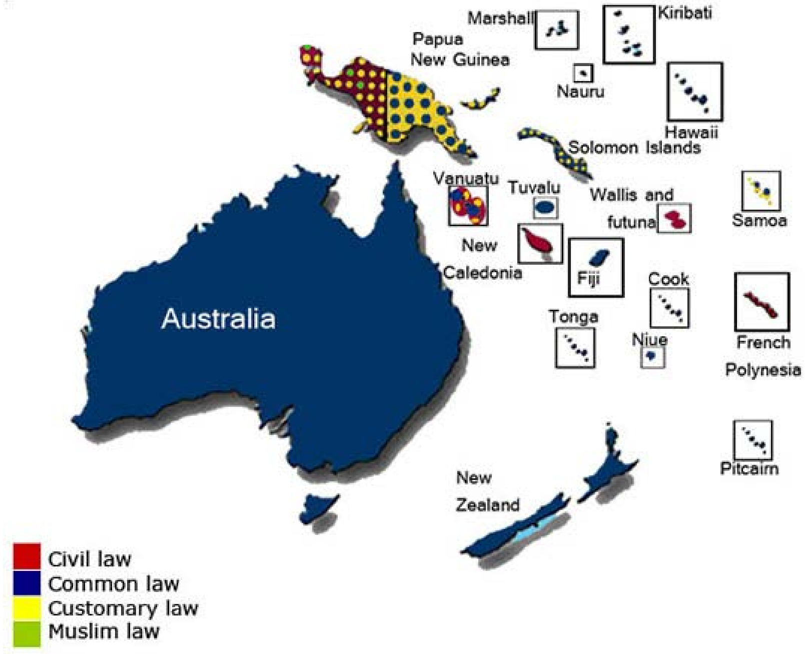
Reference:
- *CISSP® All-in-One Exam Guide*, S. Harris
- http://www.juriglobe.ca/eng/rep-geo/cartes/amer-nor

BY-NC-SA

Categories of Law …(2/4)

- Common law: Based on precedence.
  - Criminal law (imprisonment, $ penalty, etc.)
  - Civil/tort law (compensatory damage, $ restitution, no prison time.)





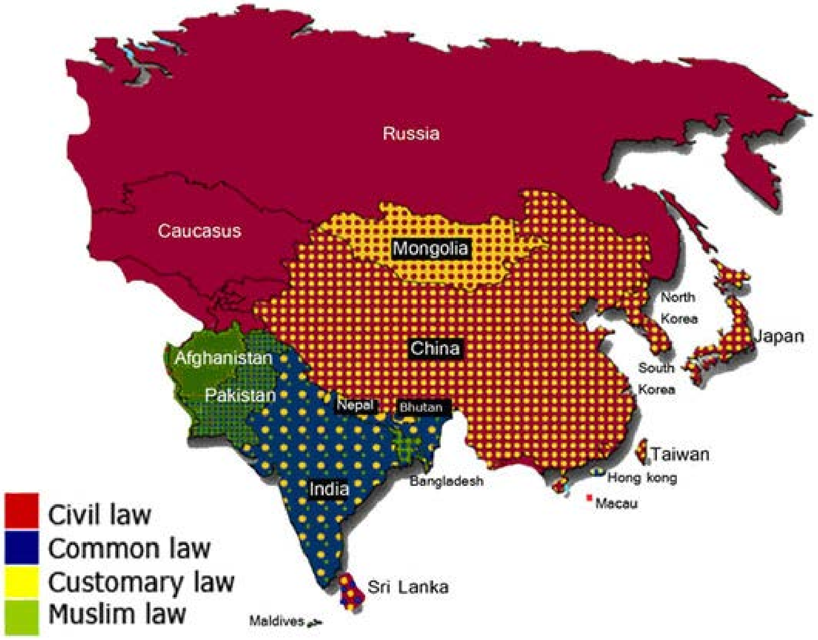
Reference:
- *CISSP® All-in-One Exam Guide*, S. Harris
- http://www.juriglobe.ca/eng/rep-geo/cartes/amer-nord.php

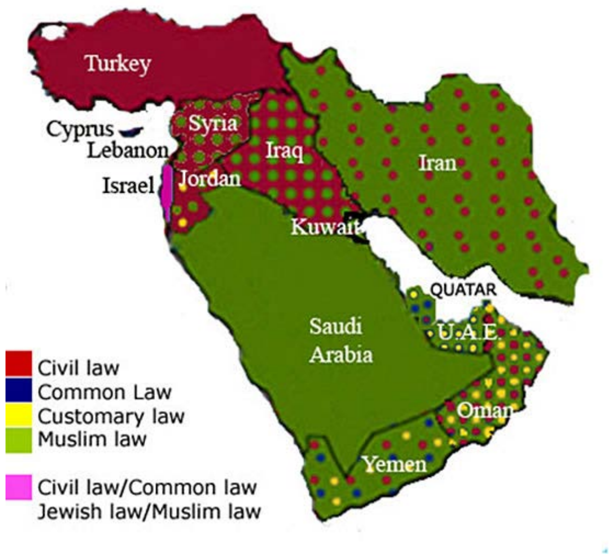
(cc) BY-NC-SA

Categories of Law ...(3/4)

- Customary law: Based on cultural customs, traditions, common believes. (ex. China, India, Muslim nations, etc.)

- Religious law: Based on religions (e.g. Islamic law)





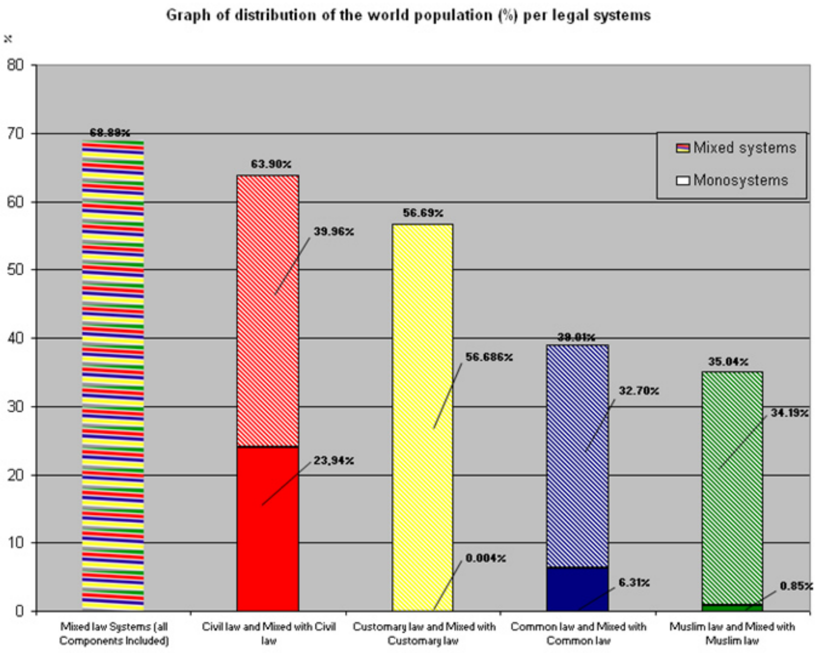
Reference: *CISSP® All-in-One Exam Guide*, S. Harris

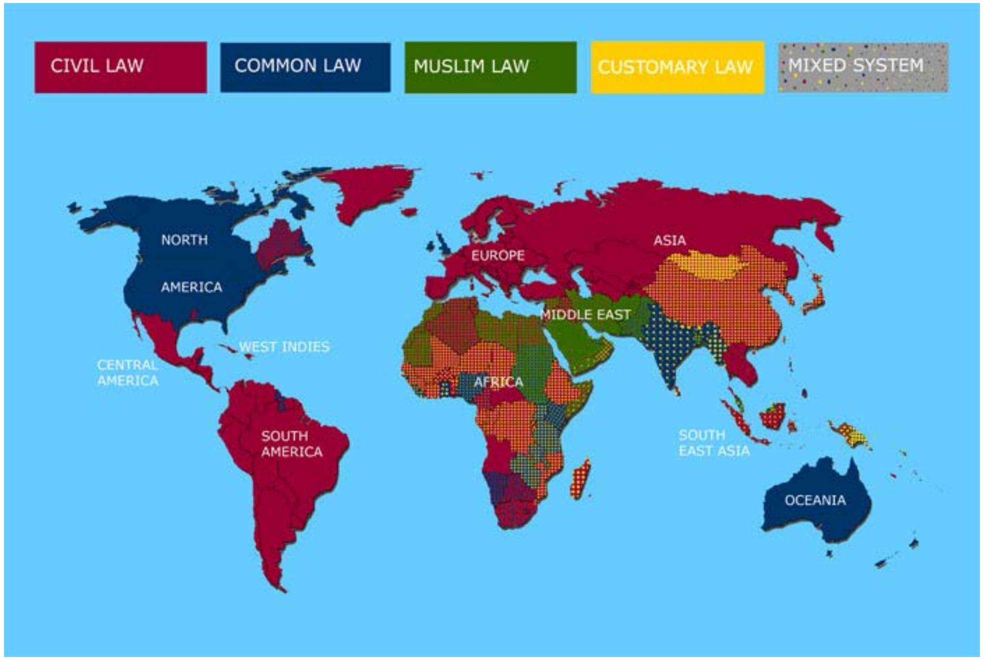
(cc) BY-NC-SA

Categories of Law …(4/4)

- Mixed law system: Based on culture, religion, & customs.
  - Civil law: Rule-based.
  - Common law: Precedence-based.
  - Customary law: Based on cultural customs, traditions, & common believes.
  - Religious law: Based on religions.

Reference:
- *CISSP® All-in-One Exam Guide*, S. Harris
- http://www.juriglobe.ca/eng/index.php





(cc) BY-NC-SA

Example of Civil Laws

- *Privacy Act of 1974*
  - Covers U.S. citizens and legal permanent residents.
  - The Government agencies must restrict disclosure of personal system of records.
  - The Government agencies must provide individuals the ability to modify their system of records.
  - Therefore, the Government agencies must establish a “code of fair information practice” policy on the collection, maintenance, disseminate and sharing of personal system of records.
- *Health Insurance Portability and Accountability Act of 1996* (HIPAA)
  - Privacy of personal medical records.
- *Electronic Communications Privacy Act of 1986* (ECPA)
  - Privacy of electronic communications. (Title I for data-in-transit, Title II for data-at-rest.)

(cc) BY-NC-SA

Privacy Act of 1974

- Individual means a citizen of the United States or an alien lawfully admitted for permanent residence.
- Record means any item, collection, or grouping of information about an individual that is maintained by an agency.
- System of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Source: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:%2B5USC552a

(cc) BY-NC-SA

What is Privacy?

- Information security is a definitive concept
  - Security Objectives: Confidentiality, Integrity, and Availability (44 USC Sec. 3542)
  - Security Implementation Principles: Need-to-know, Least Privilege, Separation-of-Duties
- “Privacy is a concept in disarray.” – Daniel J. Solove, J.D.
  - No formal definition for “privacy”, just jurisprudence
    - Bill of Rights
    - Federal privacy statues
    - State privacy statues
  - Sociological Concept: “The need for privacy is a socially created need. Without society there would be no need for privacy.” – Barrington Moore, Jr.

(cc) BY-NC-SA

Classes of Privacy

- Information privacy
  - Collection and handling of personal information (medical records, credit information.)
- Bodily privacy
  - A person’s physical being and any invasion thereof (drug test, cavity search, genetic testing)
- Territorial privacy
  - Individual environment (private property, workspace, public space)
- Communications privacy
  - Correspondence between entities (e-mail, postal mail, phone conversation)

Ref: *Information Privacy – Official Reference for the CIPP*, 2007

(cc) BY-NC-SA

Privacy: Understanding of Harmful Activities – Information Collection

- Surveillance (Fourth Amendment)
  - Wiretapping
    - Need a court order (Katz vs. United States)
  - Monitoring
    - Not within a private property (Kyllo vs. United States)
    - Ok, if lack of protection (Florida vs. Riley)
    - Ok, if in public place (United States vs. Karo)
- Interrogation (Fifth and First Amendments)
  - Self Incrimination
  - Mandated Questioning
    - Not on personal affiliation to organization(s) (Shelton vs. Tucker)
    - Not on political views or associations (Baird vs. State Bar of Arizona)
    - Not on disabilities (American with Disabilities Act of 1990)
    - Not on medical / health information (CA, CT, DE, NY, WI, etc.)

(cc) BY-NC-SA

Privacy: Understanding of Harmful Activities – Information Processing

- Aggregation
  - Not ok for “rap sheet” (DOJ vs. Reporters Committee for Freedom of the Press)
  - But ok for convicted sex-offenders (Megan’s Law)
- Identification
  - President Roosevelt and Congress promised SS card would be kept confidential and not for identification purposes (Social Security Act of 1935)
  - Standard universal identifier (SUI) is not ok
- Insecurity
  - Need ways to handle and protect personal information (Fair Information Practice, Privacy Act, GLB, HIPAA, etc.)
- Secondary Use
  - Need ways to limit the secondary use (Fair Information Practice, Privacy Act, GLB, HIPAA, etc.)
- Exclusion
  - Failure to provide individuals with notice and input about their records.

(cc) BY-NC-SA

Privacy: Understanding of Harmful Activities – Information Dissemination

- Breach of Confidentiality
  - Ok, if it related to public interest (i.e., infectious disease) (Simonsen vs. Swenson)
  - Ok, if it is shared with a 3rd party (United States vs. Miller and Smith vs. Maryland)
- Disclosure
- Exposure
- Increased Accessibility
- Blackmail
- Appropriation
- Distortion

(cc) BY-NC-SA

Example of Criminal Law

- *Computer Fraud and Abuse Act of 1984* …(1/2)
  - Amended in 1994, 1996, Broadened in 2001 by the USA PATRIOT Act (P.L. 99-474, 18 U.S.C. 1030)
  - List of criminal offenses:
    - Knowingly accessing a computer without authorization to obtain national security data.
    - Intentionally accessing a computer without authorization to obtain:
      - Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.
      - Information from any department or agency of the United States.
      - Information from any protected computer if the conduct involves an interstate or foreign communication.
    - Intentionally accessing without authorization a government computer and affecting the use of the government's operation of the computer.

Reference: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+18USC1030

(cc) BY-NC-SA

Example of Criminal Law

- *Computer Fraud and Abuse Act of 1984* …(2/2)
  - List of criminal offenses:
    - Knowingly accessing a computer with the intent to defraud and there by obtaining anything of value.
    - Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization.
    - Knowingly cause the transmission of a program, information, code, or command that causes damage that result in:
      - Loss to one or more persons during any one-year period aggregating at least $5,000 in value.
      - The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
      - Physical injury to any person.
      - A threat to public health or safety.
      - Damage affecting a government computer system.

(cc) BY-NC-SA

Example of Administrative Laws

- U.S. Export Administration Regulations (EAR)
  - Administered by Bureau of Industry and Security, Dep. Of Commerce (http://www.access.gpo.gov/bis/ear/ear_data.html).
  - EAR, Part 774, Category 5 (Part 2) – *Information Security*: mass market & retail cryptography can be exported without a license.

- European Union Council (EC) Regulation No. 1334/2000 (22 June 2000): *Setting up a Community Regime for the Control of Exports of Dual-use Items and Technology*
  - Member states can issue General Intra-Community Licenses to export crypto products within EU.
  - Export to non-EU countries require a Community General Export License (CGEA) or General National License.

Reference: *Official (ISC)^{2}® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Intellectual Property Laws

Intellectual property is divided into two categories:

- Industrial property
  - Inventions (patents),
  - Trademarks,
  - Industrial designs, and
  - Geographic indications of source.

- Copyright
  - Literary works (e.g. books, articles, architecture designs, engineering designs, plays, poems, etc.)
  - Artistic works (e.g. musical works, songs, films, paintings, photographs, sculptures, etc.)

Reference: World Intellectual Property Organization (http://www.wipo.int/portal/index.html.en)

(cc) BY-NC-SA

Intellectual Property Laws – Industrial Property

- Patent
  - A patent grants the owner a legally enforceable right to exclude others from practicing the invention covered.
  - Usually 20 years from the filing date.
- Trademark
  - Word, name, symbol, color, sound, product shape or combination of these used to identified goods & distinguish them from those made or sold by others.
  - When a trademark is used in relation to services rather than products, it may sometimes be called a "service mark".

Reference:

- *Official (ISC)²® Guide to the CISSP® CBK*
- *General Information Concerning Patents*, USPTO (http://www.uspto.gov/patents/resources/general_info_concerning_patents.jsp#heading-3)

(cc) BY-NC-SA

Intellectual Property Laws - Copyright

- Copyright
  - Is a set of exclusive rights regulating the use of a particular expression of ideas (i.e. “original works of authorship”).
  - Copyright law covers only the form or manner in which ideas or information have been manifested, the "form of material expression".
  - It is not designed or intended to cover the actual idea, concepts, facts, styles, or techniques which may be embodied in or represented by the copyright work
- Trade Secrets
  - Proprietary business or technical information which is confidential and protected as long as its owner takes “reasonable” security precautions.
  - Not a formal protection; a third party is not prevented from independently duplicating and using the secret information once it is discovered.
  - It does not expire as would a patent.

Reference: *Official (ISC)²® Guide to the CISSP® CBK*

(cc) BY-NC-SA

Information Security Related Legal Issues

Three types of harm addressed in computer crime laws:

- Unauthorized access.
- Unauthorized alteration, destruction or disclosure of information.
- Insertion of malicious programming code.

Three categories of computer crime:

- Computer assisted crime (computer as a tool).
- Computer targeted crime (crime directed at computer).
- Computer is incidental (computer data from criminal activities).

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Computer Crime Law Issues

- Defining electronic information or data.
- Defining intellectual property.
- Complex legal definitions of technical issues.
- Unlawful destruction of data or denial of service.
- Using a computer to commit, aid, or abet crime.
- Private sector lack of reporting.
- Sentencing guidelines (for “white-collar” crimes).

Reference: *Official (ISC)^{2}® Guide to the CISSP® Exam*

(cc) BY-NC-SA

International Computer Crime Law Issues

- Some countries have no or poorly defined computer crime laws.
- Law enforcement technical capabilities vary.
- Government may not wish to assist each other in international cases.
- Trans-national criminal activities.
- Jurisdictional legal disputes.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

(cc) BY-NC-SA

International Groups addressing Computer Crimes

- The G8 Nations: International agreements on computer crime.
- Mutual Legal Assistance Treaties (MLAT): U.S. law enforcement agents (i.e. FBI, Department of State) working with law enforcement of other nations.
- European Union Border Controls (Interpol): International police organization.
- United Nations (U.N.): U.N. Agreements.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

(cc) BY-NC-SA

Example of International Treaties – Export Control

- Coordinating Committee for Multilateral Export Controls (COCOM)
  - 17 member nations, dissolved in March 1994.
  - Maintained International Industrial List & International Munitions List. To prevent export of cryptography to "dangerous" countries.
- Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1995)
  - December 1998, 33 nations has agree to restrict export of crypto products based on key length. (56-bit for symmetric, 512-bit for asymmetric)
  - Products that use encryption to protect intellectual property (e.g. DVDs) is relaxed.
  - Export of all other crypto require license.

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Example of International Treaties – Export Control

- Export control of cryptosystems:
  - EAR, Part 774, Category 5 (Part 2) – *Information Security*: mass market & retail cryptography can be exported without a license.
    - Parity bits are not included in the key length
    - Key length of 56-bit for symmetric (DES)
    - Key length of 512-bit for asymmetric (RSA, Diffie-Hellman)
    - Key length of 112-bit for ECC-DH
  - European Union Council (EC) Regulation No. 1334/2000 (22 June 2000): *Setting up a Community Regime for the Control of Exports of Dual-use Items and Technology*
    - Parity bits are not included in the key length
    - Key length of 56-bit for symmetric (DES)
    - Key length of 512-bit for asymmetric (RSA, Diffie-Hellman)
    - Key length of 112-bit for ECC-DH

(cc) BY-NC-SA

Example of International Treaties – Cybercrime Definition

- On August 3, 2006, U.S. Senate signed the first international treaty on computer crime – *Council of Europe Convention on Cybercrime*.
  - Negotiations on the treaty began in 1997.
  - Final document ratified by 15 European nations and the United States.
  - U.S. Senate did not consider the optional: *Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems* due to our First Amendment – Freedom of Speech.

Reference:

- http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
- http://www.cybercrime.gov/

(cc) BY-NC-SA

International Issues on Intellectual Property (IP) …(1/2)

- On patents… (http://www.wipo.int/treaties/en/registration/pct/summary_pct.html)
  - Covered by Patent Cooperation Treaty (PCT) of 1978.
  - Not for "all" nations. (141 nations as of March 7, 2009.)
  - Not implemented in uniform manner:
    - China has never signed PCT. However, China has signed Washington Treaty in May 1990. An only applies to Hong Kong and Macao Special Administrative Regions.
    - Taiwan enforces PCT, but is not a recognized state, so it can't sign treaties.
- On copyright…
  - "There is no such thing as an 'international copyright' that will automatically protect an author's writing throughout the world." – U.S. Copyright Office (http://www.copyright.gov/fls/fl100.html).
  - Covered by Berne Convention, enforced by 164 nations.
  - Not implemented in uniform manner:
    - Paris Convention of 1992 only applies to Hong Kong and Macao Special Administrative Regions.

(cc) BY-NC-SA

International Issues on Intellectual Property (IP) …(2/2)

- In 2005, U.S. intellectual property is estimated worth between $5 – $5.5 trillion, which accounts for 45% of GDP. – *Intellectual Property Book*, GIPC, U.S. Chamber of Commerce, 2010.
- “Software piracy costs U.S. software companies billions of dollars each year.” – R. Holley, Business Software Alliance testified before House Foreign Affairs Committee on March 10, 2010.
- On October 2009, China issued its own “exclusive right” laws on patents and trademarks.
  - Foreign companies must provide their trade secrets in order to sell any products developed overseas to Chinese government.
  - Foreign companies are challenged by Chinese companies based on their Chinese issued patents

– D. Roberts, China: Closing for Business?, Bloomberg Businessweek, March 25, 2010.

(cc) BY-NC-SA

Questions:

- What are the three categories of computer crime?
  - –
  - –
  - –

- Why international computer crime law do not apply to “all nations”?
  - –

- What is the difference between copyright and trade secret?
  - –
  - –

(cc) BY-NC-SA

Answers:

- What are the three categories of computer crime?
  - Computer assisted (i.e., computer as a tool)
  - Computer targeted (i.e., computer is the target)
  - Computer is incidental (i.e., data in a criminal activities)

- Why international computer crime law do not apply to “all nations”?
  - Nation is a sovereign entity, law of one nation does not apply to another nation unless there is a treaty that acknowledges the computer crime law.

- What is the difference between copyright and trade secret?
  - Copyright is a set of exclusive rights.
  - Trade secret has no formal protection, it is a “proprietary” information.

(cc) BY-NC-SA

Topics

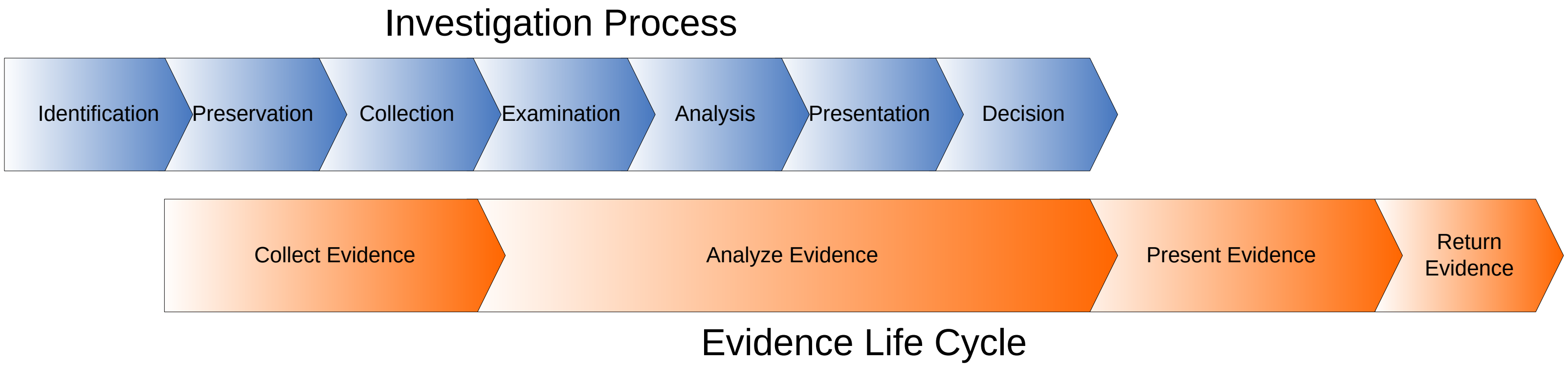
Legal, Regulations, Compliance and Investigations Domain

- Laws & Regulatory Compliance
- ➡ Investigations & Digital Forensics
- Ethics

(cc) BY-NC-SA

Investigative Process vs. Evidence Life Cycle

- Investigative Process encompasses
  - Identification of an incident
  - Preservation of “scene”
  - Collection of evidence
  - Examination of evidence
  - Analysis of the incident
  - Presentation of evidence
  - Decision to act
- Evidence Life Cycle
  - Acquisition collection and identification
  - Storage, preservation, and transportation
  - Analysis
  - Presented in court
  - Returned to victim



Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

(cc) BY-NC-SA

Data Acquisition – Preservation of Forensic Evidence

- Make 2 copies of the original media (Primary Image / Working Image).
- Bit for Bit copying capture all the data on the copied media including hidden and residual data (e.g. slack space, swap, residual, unused space, deleted files, etc.)
- Preserve integrity of source and image (e.g. hash functions)
  - MD-5 sum provides a 128-bit signature that is sensitive to bit changes.
  - The reported digest should match.

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Rule of Evidence

- Type of evidence
  - Evidence is any species of proof or probative matter, legally presented at the trial of an issue, by act of parties and through the medium of witness, records, documents, objects, etc.
- Admissibility of evidence
  - Evidence must be admissible in court.
- Preservation of electronic evidence (Chain-of-custody)
  - Electronic evidence is fragile.
  - Integrity of the “scene” must be preserved.
  - Only one chance to do it correctly.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

(cc) BY-NC-SA

Rule of Evidence – Common Types of Evidence

- Direct evidence is oral testimony by witness.
- Real is physical evidence made up by tangible objects that prove or disprove guilt.
- Documentary is in form of business records, manuals, or print outs, etc.
- Demonstrative evidence is evidence used to aid the jury. In a form of model, illustration, chart or experiment offered as proof.

Reference: *Official (ISC)^{2}® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Rule of Evidence – Hearsay Rule

Hearsay is second-hand evidence; normally NOT admissible in court.

- Value depends on veracity and competence of source.
- Depending on the circumstance, business records may be considered hearsay.
  - No first-hand proof of accuracy, reliability, trustworthiness
- Business records exemption:
  - Information relates to regular business activities.
  - Automatically computer generated data.
    - No human intervention.
    - Prove system was operating correctly.
    - Prove no one changed the data.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

(cc) BY-NC-SA

Rules of Evidence – Admissibility of Evidence

- Relevancy of evidence
  - Proof a crime occurred.
  - Document of events & time frame.
  - Identification of acts / methods.
  - Sources of evidence: Oral (witnesses), Written Document, Computer generated, Visual/audio (during & after events).
- Reliability of evidence
  - Evidence is Trustworthy.
  - Evidence is legally obtained.
- Durability of evidence
  - Evidence identification & preservation
  - Preservation, collection and documentation (Chain-of-custody)
  - Can be reconstructed

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Rule of Evidence – Handling of Computer Evidence

- Minimize handling/corruption of original data.
- Account for any changes and keep detailed logs of your actions.
- Comply with the rules of evidence.
- Do not exceed you knowledge, seek legal advise.
- Follow you local security policy and obtain written permission.
- Capture as accurate an image of the system as possible.
- Be prepared to testify.
- Ensure you actions are repeatable.
- Proceed from volatile to persistent evidence.
- Don’t run any programs on the affected system.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

(cc) BY-NC-SA

Rule of Evidence – Chain of Custody

- Helps protect the integrity and reliability of the evidence.
- Effective process of documenting the complete journey of the evidence during the life of the case.
- To answer the following questions:
  - Who collected it?
  - How & where?
  - Who took possession of it?
  - How was it stored & protected in storage?
  - Who took it out of storage & why?

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP® Exam*

(cc) BY-NC-SA

IOCE-G8

- In March 1998, the International Organization on Computer Evidence (IOCE) was appointed by U.N.: (http://www.ioce.org)
  - To define international principles for the procedures relating to digital evidence,
  - To ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state.
- IOCE principals are governed by the following objectives: (i.e., by-laws)
  - To identify and discuss issues of common interest
  - To facilitate the international dissemination of information
  - To develop recommendations for consideration by the member agencies

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

(cc) BY-NC-SA

IOCE-G8 – Principles of Computer Evidence

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied
- Upon seizing digital evidence, actions taken should not change that evidence
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
- All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review
- An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession
- Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles

Reference: *Official (ISC)²® Guide to the CISSP® Exam*

(cc) BY-NC-SA

Digital Forensics

- While digital forensics has been around for a while; they are still a bit of “CSI black art”. For CISSP, it consists of:
  - Media analysis
  - Network analysis
  - Software analysis
  - Hardware/embedded device analysis

- There are much more…
  - Cryptographic analysis
  - Steganography analysis
  - Audit trails analysis
  - Digital watermarks

(cc) BY-NC-SA

Digital Forensics – Media Analysis

- There are all types of storage media…

- They all use some type of standard digital format
  - Do the “bit-for-bit” copy and hash it.
  - Maintain “chain-of-custody” and preserve the original evidence
- Most of time, forensic analysts look for incriminating data:
  - Web browsing history, cookies, user id, passwords
  - Data files: document, spreadsheet, pictures, etc.
  - Log files: system, application
  - Hidden, temporary, and deleted files
  - E-mails, contact information
- If encrypted, then do the cryptographic analysis

(cc) BY-NC-SA

Digital Forensics – Software Analysis

- Software applications can write data just about everywhere…
  - Web browser: browsing history, cookies, and temporary files
  - OS: log, swap files, deleted files, print spool files
  - Applications: temporary files, e-mail (.pst files), encrypted, steganography, etc.
  - Malware: Trojan-horse executable, logs, unallocated space (hidden blocks), boot sectors, slack space, etc.
- Forensic toolkits such as: Forensic Toolkit and EnCase helps, but still requires experience and analytical mind.

BY-NC-SA

Digital Forensics – Network Analysis

- Capture of network data:
  - Full packet capture
  - Data flow
  - Security alert data and logs

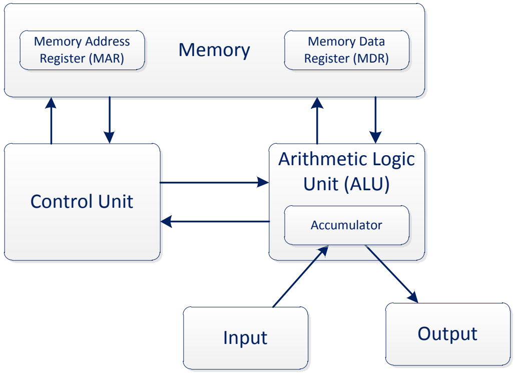
- Capture of network data is done using tools such as:
  - PCAP
  - Netwitness, NetFlow, IPFIX, etc.
  - Log files from firewall, IPS/IDS, routers, switches, etc.

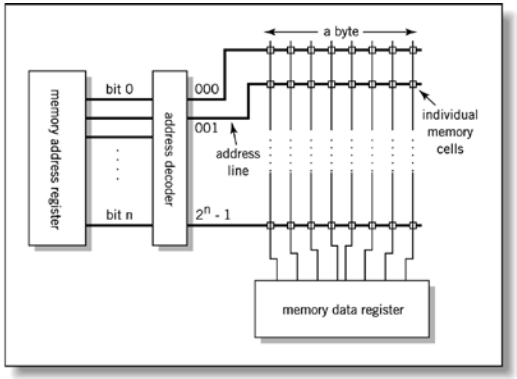
- Analysis of captured network data is done using:
  - Wireshark, TCPDump
  - Netwitness, SiLK, Argus, etc.
  - SIEM tools: Arcsight, RSA enVision, Splunk, etc.

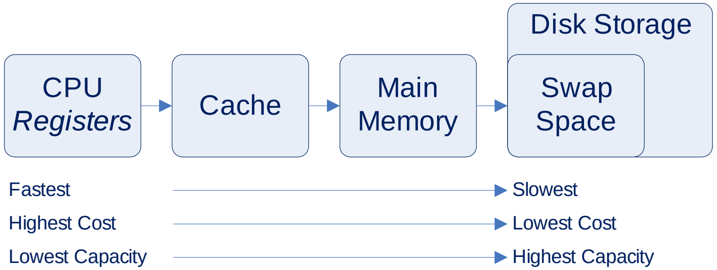
(cc) BY-NC-SA

Digital Forensics – Hardware/Embedded Device Analysis

- Hardware/embedded device analysis is most challenging and requires:
  - Deep knowledge of how computer works (i.e., von Neuman computer architecture, memory registry, IO drivers.)


Memory Address Register (MAR)
Memory
Memory Data Register (MDR)
Control Unit
Arithmetic Logic Unit (ALU)
Accumulator
Input
Output





  - Requires deep knowledge of assembly language and assembler.
  - Typically “platform-specific, system-on-chip”: Intel x86, AMD, ARM, Intel Atom, etc.
  - ICS/SCADA are mostly “purpose-build” platforms using proprietary architecture.

(cc) BY-NC-SA

Digital Forensic Analysis @ MITRE

- Xeno Kovah (G029) & friends have several training courses on digital forensics: Online at http://opensecuritytraining.info/Welcome.html
  - Introductory & Intermediate Intel x86: Architecture, Assembly, Applications, and Alteration
  - The Life of Binaries
  - Malware Dynamic Analysis
  - Introduction to Network Forensics
  - Android Forensics & Security Testing
  - Rootkits: What they are, and how to find them
  - Reverse Engineering Malware

- MITRE Institute:
  - TSV108: Introduction to Computer Forensics: Hard Disk Media Analysis (Rick Murad [G027])
  - TSV049: Identifying, Obfuscated and Forensic Techniques for Web User Identification (Zak Zebrowsk [G122])

(cc) BY-NC-SA

Incident Response – CSIRT

- Computer Security Incident Response Team (CSIRT) a.k.a.:
  - Computer Emergency Response Team (CERT)
  - Security Operations Center (SOC)
- CERT® started as a DARPA program in November of 1988, after the Morris worm incident.
  - Similar to MITRE, CERT Coordination Center (CERT/CC) is a FFRDC managed by the Software Engineering Institute of Carnegie Mellon University (CMU/SEI)
  - Areas of Work:
    - Software Assurance
    - Secure Systems
    - Organizational Security
    - Coordinated Response (e.g., CSIRTs)
    - Education and Training

(cc) BY-NC-SA

Reference: http://www.cert.org/meet_cert

Incident Response – Categories of CSIRT Services

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

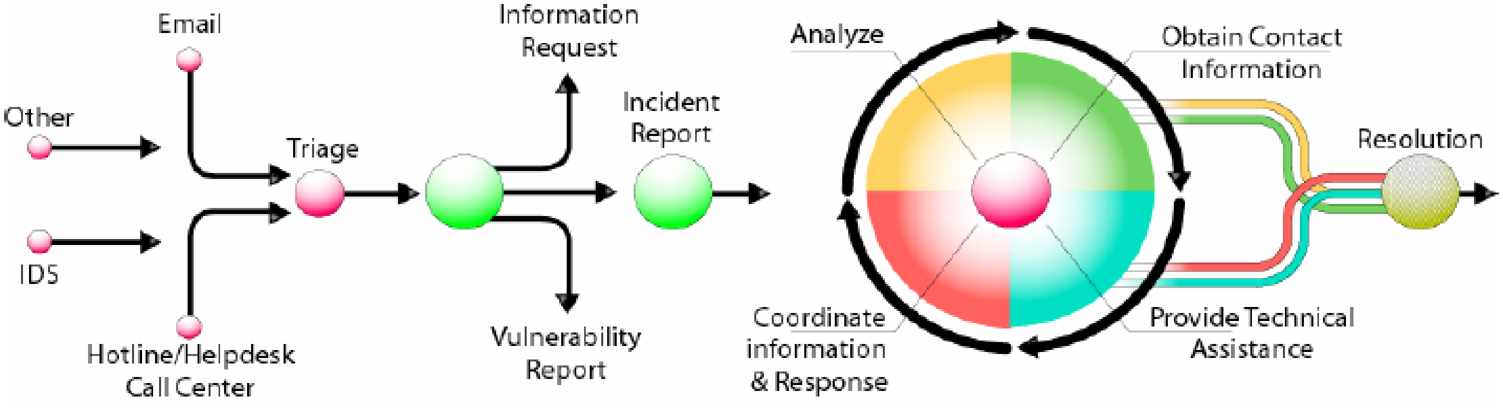
- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Reference: *Handbook for Computer Security Incident Response Teams (CSIRTs)*, CMU-SEI

(cc) BY-NC-SA

Incident Response

- Observe event(s) → Identify incident.
- Triage:
  - – Contain damage and Preserve & Collect evidence .
  - – Document incident and escalate to CSIRT.
- CSIRT examine evidence and conduct analysis on incident.
- Generate mitigation steps and coordinate response measures.


Email
Other
IDS
Hotline/Helpdesk Call Center
Triage
Information Request
Incident Report
Vulnerability Report
Analyze
Obtain Contact Information
Resolution
Coordinate information & Response
Provide Technical Assistance

Reference: *Handbook for Computer Security Incident Response Teams (CSIRTs)*, CMU-SEI

(cc) BY-NC-SA

Questions:

- What type of evidence is the oral testimony by a witness?
  - –

- What type of evidence is where it is presented to jury in a form of model, illustration, chart or experiment outcome?
  - –

- What type of business record is exempt from the hearsay rule?
  - –

(cc) BY-NC-SA

Answers:

- What type of evidence is the oral testimony by a witness?
  - Direct

- What type of evidence is where it is presented to jury in a form of model, illustration, chart or experiment outcome?
  - Demonstrative

- What type of business record is exempt from the hearsay rule?
  - Auto-generated computer data related to regular day-to-day business activities.

(cc) BY-NC-SA

Questions:

- What is the best practice for preserving electronic evidence?
    –

- What are the three criteria of an admissible evidence?
    –
    –
    –

(cc) BY-NC-SA

Answers:

- What is the best practice for preserving electronic evidence?
  - Bit-for-bit copy with an associated digest.

- What are the three criteria of an admissible evidence?
  - Relevancy
  - Reliability
  - Durability

(cc) BY-NC-SA

Topics

Legal, Regulations, Compliance and Investigations Domain

- Laws & Regulatory Compliance
- Investigations & Digital Forensics
- Ethics

(cc) BY-NC-SA

Concept

Ethics vs. Law

- Ethics is “Should”,
- Law is “Must”.

(cc) BY-NC-SA

RFC 1087, Ethics and the Internet

Internet Activities Board (IAB) characterized the following activities as unethical and unacceptable on the Internet:

a) Seeks to gain unauthorized access to the resources of the Internet,

b) Disrupts the intended use of the Internet,

c) Wastes resources (people, capacity, computer) through such actions,

d) Destroys the integrity of computer-based information, and/or

e) Compromises the privacy of users.

(cc) BY-NC-SA

(ISC)^2 Code of Ethics

Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is condition of certification.

Reference: *(ISC)$^{2®}$ Code of Ethics*

(cc) BY-NC-SA

(ISC)^2 Code of Ethics

Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

(cc) BY-NC-SA

(ISC)^2 Code of Ethics – Canons

Protect society, the commonwealth, and the infrastructure.

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Reference: *(ISC)$^{2®}$ Code of Ethics*

(cc) BY-NC-SA

(ISC)^2 Code of Ethics – Canons

Act honorably, honestly, justly, responsibly, and legally.

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Given prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Reference: *(ISC)$^{2®}$ Code of Ethics*

(cc) BY-NC-SA

(ISC)^2 Code of Ethics – Canons

Provide diligent and competent service to principals.

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Reference: *(ISC)$^{2®}$ Code of Ethics*

(cc) BY-NC-SA

(ISC)² Code of Ethics – Canons

Advance and protect the profession.

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these cannons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

Reference: *(ISC)²® Code of Ethics*

(cc) BY-NC-SA

Ethics Plan of Action

- Develop a corporate guide to computer ethics for the organization
- Develop a computer ethics policy to supplement the computer security policy
- Add information about computer ethics to the employee handbook.
- Find out whether the organization has a business ethics policy, and expand it to include computer ethics.
- Learn more about computer ethics and spread what is learned.

Reference: *Official (ISC)$^{2®}$ Guide to the CISSP$^{®}$ Exam*

(cc) BY-NC-SA