CISSP Domain 1 — Security and Risk Management

Domain 1 — Security and Risk Management

References to ISO standards and NIST documents begin in this domain and continue throughout the rest of the domains. You need to compile a set of lists for your study guide. I put them all here, along with lists of regulations.

The example I always use: to be culturally aware, you should know that the *Torah* is the scripture of Judaism, the *Quran* is the scripture of Islam, the *Vedas* are the scripture of Hinduism, and so on. You don't have to actually read any of them to know that. **Nor should you read any of the following documents.** Just be able to match their names or numbers to what they're about.

Yellow means very likely to appear on exam, grey means less likely, not colored means medium likelihood, *all of these being my best guess, what I would use if I had to re-take the exam.*

ISO Standards

ISO 15026	*Systems and Software Engineering*
ISO 15288	*Systems and Software Engineering*
ISO 17889	Defines cloud computing, like NIST plus NaaS or Network-as-a-Service.
ISO 27000	Not mentioned much, seems to be more or less a dictionary.
ISO 27001	*Information Security Management System,* defines what "secure" means.
ISO 27002	Guidance and best practices to make ISO 27001 happen.
ISO 27005	Information Security Risk Management.
ISO 31000	Risk Management — Principles and Guidelines.

NIST Documents

SP 800-37	Risk Management Framework
SP 800-53	Catalog of security and privacy controls (security toolkit)
SP 800-60	Guide to Mapping Types of Information and Information Systems to Security Categories
SP 800-63	How to do identity proofing and registration
SP 800-88	Guidelines for Media Sanitization
SP 800-160	System Security Engineering

FIPS

U.S. Government **Federal Information Processing Standards.**

FIPS 140-2	Certifies cryptographic software and hardware. Four levels of increasing security: 1. FIPS 140-2 Level 1 = correct implementation 2. FIPS 140-2 Level 2 = tamper-evident 3. FIPS 140-2 Level 3 = tamper-resistant 4. FIPS 140-2 Level 4 = automatic zeroizing, strongly tamper-resistant even in a sophisticated lab environment
FIPS 199	Categorizes U.S. federal information based on the impact of violations of its confidentiality, integrity, and availability.
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*

SCAP, OVAL, and STIGs

U.S. NIST created SCAP, a protocol *and* standards and nomenclature for testing and reporting on software vulnerabilities and configuration problems.

XCCDF and OVAL are reporting formats and languages.

CPE, CCE, CVE (and others) are enumerations defined by MITRE on behalf of the U.S. Government. CVSS and CCSS are related vulnerability scoring systems.

NVD or National Vulnerability Database is managed by NIST.

Other Standards and Documents and Groups

COBIT	**How to manage and document** enterprise IT and IT security functions.
COSO	Formed in response to dramatic and severe **financial industry scandals** in the U.S. in the 1980s, to address financial reporting irregularities and fraud.
CSA STAR	An organization's **list of cloud service providers** with tiers: 1. "We're secure because we did a questionnaire so trust us." 2. Assessed by an external auditor certified by CSA. 3. Continuously monitored, maybe about to finally arrive in late 2019.
ENISA	Network of network and information **security expertise for the E.U.,** its member states, and its private sector and citizens.
ICASA	Publishes IT RISK framework, **connects strategic business perspective with IT** management.
ITIL	**A service delivery set of best practices,** focused on **business goals.**
ITU	Internal **Telecommunication** Union — standardizes communication technologies.
Uptime Institute	Certification for **data centers,** advice on their **design.**

Regulations

The (ISC)^2 CCSP certification goes into further details on these. This includes how the E.U. GDPR is quite strict. And several countries already had, or soon enacted, privacy laws at least as strict as GDPR, so E.U. data can easily be exported to them for processing: Australia, New Zealand, Argentina, Japan, Switzerland, and some others.

APEC (or Asia-Pacific Economic Cooperation) is East Asian countries wanting to be secure enough to do business without getting in the way of the business itself. If you've seen Hong Kong business, from neon-lit glass towers to the night markets, this is easy to remember.

Hong Kong

The OECD helps governments and organizations around the world deal with improving economic and social well-being, it also balances privacy with profit.

Meanwhile, the U.S. continues to have absolutely *no* guarantee of privacy. **Safe Harbor** got no respect, its replacement **Privacy Shield** wasn't much better. U.S. companies manage to do international business with specific contract clauses promising E.U.-level protection.

FedRAMP	U.S. federal requirement connected to FISMA, regulating the purchase and use of cloud and other managed IT services.
FISMA	U.S. federal law applying only to Government agencies, requiring them to comply with NIST standards.
GDPR	E.U. **strict** requirements for privacy, as international law.
GLBA	U.S. federal law requiring banks to protect customer data.
HIPAA	U.S. federal law about health-related personal information.
PIPEDA	Canadian federal requirement to protect personal privacy.
Sarbanes-Oxley a.k.a. Sarbox, SOX	U.S. federal requirements created in response to dramatic financial frauds in the 1990s.

Legal Concepts

This is a shortened list of what I have on the corresponding CCSP study guide. I don't know exactly how much shows up, I'm probably erring on the side of caution with too much. **This set is more likely to show up.**

- **Due Care** versus **Due Diligence**
  - **Due Diligence** — **Investigating and planning,** done in advance.
  - **Due Care** — **Conduct that a reasonable and prudent person with proper training will exercise,** careful ongoing operations.
- **Criminal law** is government vs persons, groups, or organizations violating statutes. **Conduct prohibited by the government,** protecting safety and well-being of the public. Penalties can be monetary, prison time, or even death. **Requires proof "beyond a reasonable doubt",** very small chance it's not true.
- **Civil law** governs **private citizens and their disputes.** Parties are strictly private entities including individuals, groups, and organizations. Could be a breach of contract with cloud service provider. Penalties are monetary, or court-ordered relief such as property of the performance of activities. **Requires "a preponderance of evidence",** more likely true than not.

- **Tort law** — Part of civil law, "a body of rights, obligations, and remedies" setting out **reliefs for persons suffering harm as a result of wrongful acts of others.** The individual who committed the wrongful act is liable for the costs and consequences of it, not the victim. Don't require a prior agreement between the parties.
- Criminal vs tort vs civil:
  - Criminal: Prosecuting attorney says "He stole PHI and sold it for fraud, extortion, and identity theft."
  - Tort: Patient says "The hospital did not exercise Due Care, my PHI was inadequately protected."
  - Civil: Hospital says "That company did not process our data correctly, despite our contract."

Legal Terms

This is a shortened list of what I have on the corresponding CCSP study guide. I don't know exactly how much shows up, I'm probably erring on the side of caution with too much. **This set is less likely to show up, but still possible.**

- **Warrant:** Issued to law enforcement by a judge on presentation of probable cause, enforces the arrest of an individual or seizure of property.
- **Subpoena:** Issued by an attorney with a material interest in the case. The subpoena is "issued by an officer of the court", must be obeyed like a warrant.
- **Doctrine of plain view:** In some U.S. states, a law enforcement officer may seize evidence without a search warrant if they can see it without making entry.
- **Doctrine of the silver platter:** When you hand over unneeded data in the production step, too much, and some might get used against you.
  - Policeman pulls you over, sees a bloody ax in the back seat = doctrine of plain view
  - Policeman pulls you over, you ask "Don't you want to look in my trunk?" = doctrine of the silver platter
- **Extradition:** One country transfers a suspected or convicted criminal to another country, assuming:
  - Act is a crime punishable in both countries
  - Countries have an extradition treaty
  - Penalty or punishment is generally equal in both countries
- **Harmonization of law:** Creating common legal standards across the EU.
- Preparing for legal actions:
  - **Legal hold:** When a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and ensure the preservation of relevant documents.
  - **E-Discovery:** Any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence.
  - **Spoliation:** The intentional or accidental destruction or alteration of data either on “legal hold” or lawfully requested.
  - **Production:** Presenting the requested data to the court or requesting party.

Roles

A hospital provides a useful setting for examples:

Data Subject — the person to whom the sensitive data refers.
The patient.

Data Owner / Data Controller — the entity that collects or creates the sensitive information, **legally accountable for its protection.**
CEO or the board of directors of the hospital.
The same people, you think of them as Controller when they are planning what data to collect and why, and as Owner when considering legal accountability.

Data Steward — responsible for data content, context, and the associated business rules.
Head of medical records, selects data and metadata, formats, procedures for data entry. Nurses and radiology technicians follow the Steward's procedures.

Data Custodian — manages the data day-to-day on behalf of the owner / controller.
System administrators, database administrators, backup operators, and other IT staff at the hospital.

Data Processor — enters or manipulates or transforms or otherwise processes the sensitive data, on behalf of the owner / controller.
Contractor transcribing physician notes, submitting health insurance claims, etc.

Due Diligence / Due Care

Due Diligence is investigation and planning carried out initially. It supports...

Due Care is an *ongoing process* maintaining what a well-informed, skilled, prudent person would do for their customer.

Quantitative Risk Analysis

This is elementary school analysis and math, dressed up with fancy terms and acronyms.

You have an asset that brings in $100,000 per year. A web site selling something, let's say.

A specific attack might take away 10% of that.

Given past experiences and current defenses, you estimate that the attack will probably happen once every 4 years, on average.

So, to quantitatively analyze that risk:

AV or the **Asset Value** is $100,000.

EF or the **Exposure Factor** is 10% or 0.1.

The **SLE** or **Single Loss Expectancy** is how much one successful attack costs. Its total value times the fraction lost, duh.
SLE = AV × EF
SLE = $100,000 × 0.1
SLE = $10,000

The **ARO** or **Annual Rate of Occurance** is the number of times it's expected to happen in a typical year. Once every four years means 0.25 per year.

The **ALE** or **Annual Loss Expectancy** is, duh, how many times it's expected to happen in a year times how much each event costs.
ALE = SLE × ARO
ALE = $10,000 × 0.25
ALE = $2,500

Then, make sure that defenses don't cost more than that per year. Don't spend a dollar to save a nickel.

STRIDE

It's a contrived acronym:
Spoofing identity,
Tampering with data,
Repudiation, Information disclosure,
Denial of service,
Elevation of privilege

Octave

From CMU, for viewing overall risk across an organization — *less likely to appear on test.*

DLP vs DRM

DRM protects intellectual property.
You can't watch this DVD. Even though you've seen the movie dozens of times and contributed to the Wikipedia article describing it in detail.

DLP protects secrets.
This document can't leave headquarters. It's the script for the next movie in the series, which is about to start filming.

Education, Training, Awareness

Education	Formal classes, usually at an accredited academic institution.
Training	1-to-5 day courses presented by subject matter experts, usually working for for-profit training providers.
Awareness	Informal, short, to remind and encourage employees.