FRSecure CISSP Mentor Program

2023

Class #2 - Introduction

Brad Nigh
FRSecure

CISSP® MENTOR PROGRAM – SESSION TWO

WELCOME

Now it get's real!

We have a lot to cover tonight, but no worries. Mostly the basics!

BUT before we dive in...

CISSP® MENTOR PROGRAM – SESSION TWO

WELCOME

Now it get's real!

We have a lot to cover tonight, but no worries. Mostly the basics!

BUT before we dive in...

What do you call the boss at Old McDonald's Farm?

CISSP® MENTOR PROGRAM – SESSION TWO

WELCOME

Now it get's real!

We have a lot to cover tonight, but no worries. M

BUT before we dive in...

What do you call the boss at Old McDonald's Farm?

The CIEIO.

CISSP® MENTOR PROGRAM – SESSION TWO

WHOAMI

Brad Nigh CISM | CISSP | CMMC-RP | ITILv3

- 6th year teaching the Mentor Program
- Co-Host "The Unsecurity Podcast"

- https://www.linkedin.com/in/bradnigh/
- https://frsecure.com/unsecurity/

 @bradnigh

CISSP® MENTOR PROGRAM – SESSION TWO

BONUS!!!

[Cybersecurity Canon]

https://icdt.osu.edu/cybercanon

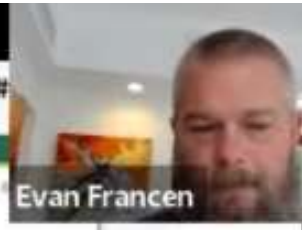
IN A "TYPICAL" CLASS...

The typical class is structured like this:

- Questions.
- Quiz.
- Current Events.
- Lecture.
- Homework (you'll appreciate the breaks...)

However, we haven't dug into the content yet, so there's no quiz tonight.

Ask questions in Discord.



CISSP® MENTOR PROGRAM – SESSION ONE

THE BOOK

Title: The Official (ISC)2 CISSP CBK Reference, 6th Edition.

- ISBN-10: 111978990
- ISBN-13: 978-1119789994

CISSP® MENTOR PROGRAM – SESSION TWO

QUESTIONS.

The most common questions since Monday have been about:

- About the Discord channel
- Live session links.
- Instructor slide deck.

Video: https://youtu.be/oUZ9ruYmfsg
(in particular, see the 55 min mark)

CISSP® MENTOR PROGRAM – SESSION TWO

QUESTIONS.

The most common questions since Monday have been about:

- **About the Discord channel**
- Live session links.
- Instructor slide deck.

Because of the way Discord works and normal communications challenges, the Discord invite you received may have "expired". Email the FRSecure CISSP Mentor List (**cisspmentor@frsecure.com**) for a new invite.

QUESTIONS.

The most common questions since Monday have been about:

- About the Slack channel
- **Live session links.**
- Instructor slide deck.

All LIVE session links will be sent by email on the same day as the LIVE session. If you have not received the live session link it's usually because the email went to your "Junk" folder (or similar).

QUESTIONS.

The most common questions since Monday have been about:

- About the Slack channel
- Live session links.
- **Instructor slide deck.**

The instructor slide decks will be sent as soon as FRSecure receives them from the instructors. Sometimes the decks are not available until they teach. Whenever possible, we will try to send you the slide decks before each class.

CISSP® MENTOR PROGRAM – SESSION TWO

CURRENT EVENTS.

There is NEVER a shortage of current events to discuss in information security!

We have a lot to cover tonight, so just one for you to consider.

CISSP® MENTOR PROGRAM – SESSION ONE

CURRENT EVENTS.

There is NEVER a shortage of current events t ity!

We hav st one for

CISSP® MENTOR PROGRAM – SESSION ONE

CURRENT EVENTS.

There is NEVER a shortage of current eve

W on

CISA added CVE-2023-28252, a Windows zero-day vulnerability in the Common Log File System (CLFS), to its catalog of Known Exploited Vulnerabilities yesterday. This flaw was first discovered in February. It's noted that this vulnerability is currently being actively exploited by cybercriminals across small and medium-sized businesses in the Middle East and North America. Threat actors have been monitored escalating privileges and deploying ransomware payloads, particularly Nokoyama.

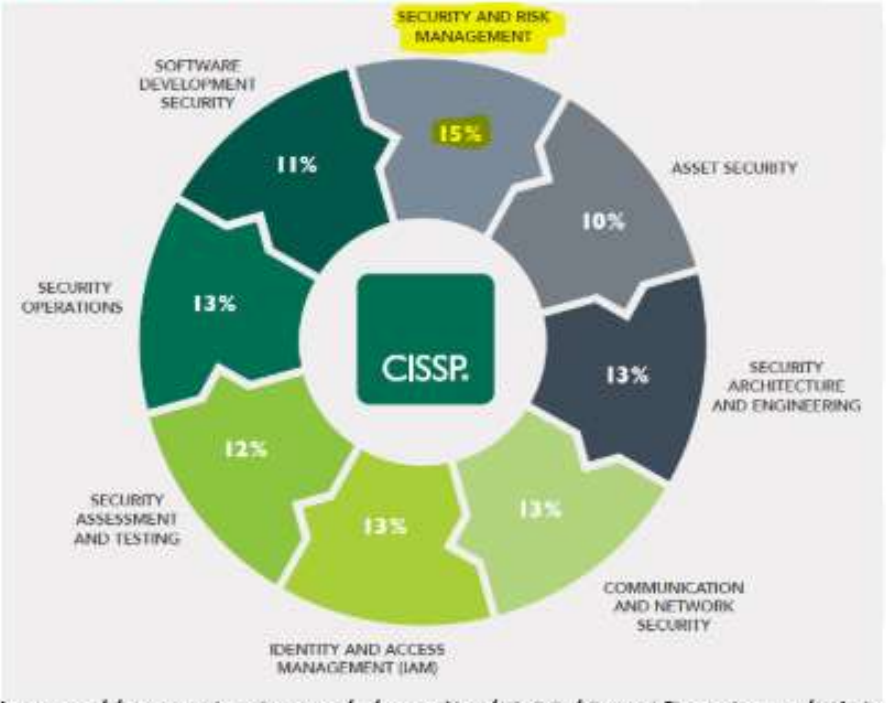
Nokoyama ransomware first surfaced in February of 2022 and was viewed as one of several offshoots of JSWorm. Since then, it has used CLFS system flaws similar to CVE-2023-28252, including in 64-bit Windows systems, to perpetrate double extortion attacks with victims' stolen data.

Microsoft patched this zero-day and 96 other bugs, including 45 remote code execution vulnerabilities, as part of April's Patch Tuesday. Full details on yesterday's patches can be found here: https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2023-patch-tuesday-fixes-1-zero-day-97-flaws/

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

CISSP Exam Overview



https://www.isc2.org/-/media/ISC2/Certifications/Ultimate-Guides/UltimateGuideCISSP-Web.ashx

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Topics:

If you read Domain 1 AND it felt a little disjointed, that's because it is (in the book).

Don't worry, we'll help it make sense!

This chapter/domain covers a bunch of basics from a bunch of places, and the course will take us deeper as we go.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Topics (Part 1 [today]):

- Understand, adhere to, and promote professional **ethics**
- Understand and apply **security concepts**
- Evaluate and apply **security governance principles**
- Determine **compliance** and other requirements
- Understand **legal and regulatory issues** that pertain to information security in a holistic context
- Understand requirements for **investigation types** (i.e., administrative, criminal, civil, regulatory, industry standards)
- Develop, document, and implement **security policy, standards, procedures, and guidelines**

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Topics (Part 2 [Next Week]):

- Identify, analyze, and prioritize **Business Continuity (BC)** requirements
- Contribute to and enforce **personnel security policies and procedures**
- Understand and apply **risk management concepts**
- Understand and apply **threat modeling concepts and methodologies**
- Apply **Supply Chain Risk Management** (SCRM) concepts
- Establish and maintain a **security awareness, education, and training program**

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Topics:

- Identify, analyze, and prioritize **Business Continuity (BC)** requirements
- Contribute to and enforce **personnel security policies and procedures**
- Understand and apply **risk m**
- Understand and apply **threa** **methodologies**
- Apply **Supply Chain Risk Ma** concepts
- Establish and maintain a **security awareness, education, and training program**

Honestly, this domain is a little all over the place and out of order.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Professional Ethics.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Professional Ethics.

- Ethics must always be a top concern for all information security professionals.
- The **(ISC)² Code of Professional Ethics** a MUST for CISSP® certification (and it is **VERY** testable).
- The code of ethics preamble is:
  - The safety and welfare of society and the common good, 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 of Ethics is a **condition of certification**.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

(ISC)² Code of Professional Ethics

- Every CISSP® member must follow.
- Governed by the (ISC)² **Code of Ethics Cannons**:
  - **Cannon I**: Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - **Cannon II**: Act honorably, honestly, justly, responsibly, and legally.
  - **Cannon III**: Provide diligent and competent service to principals.
  - **Cannon IV**: Advance and protect the profession.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

(ISC)² Code of Professional Ethics

- Every CISSP® member must follow.
- Governed by the (ISC)² **Code of Ethics Cannons**:
  - **Cannon I**: Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - **Cannon II**: Act honorably, honestly, justly, responsibly, and legally.
  - **Cannon III**: Provide diligent and competent service to principals.
  - **Cannon IV**: Advance and protect the profession.

The cannons are ordered by importance. Make sure you understand your employer's code of ethics too (if there is one).

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

According to the CISSP Certification Exam Outline, the subtopics are "Confidentiality, integrity, and availability, authenticity and nonrepudiation"

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

According to the CISSP Certification Exam Outline, the subtopics are "Confidentiality, integrity, and availability, authenticity and nonrepudiation"

These are all VERY important; however, let's simplify things for a second.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

According to the CISSP Certification Exam Outline, the subtopics are "Confidentiality, integrity, and availability, authenticity and nonrepudiation"

These are all VERY important; however, let's simplify things for a second.

What is our definition of "**information security**"?

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

According to the CISSP Certification Exam Outline, the subtopics are "Confidentiality, integrity, and availability, authenticity and nonrepudiation"

These are all VERY important; however, let's simplify things for a second.

What is our definition of "**information security**"?

It doesn't get any simpler.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

According to the CISSP Certification Exam Outline, the subtopics are "Confidentiality, integrity, and availability, authenticity and nonrepudiation"

These are all VERY important; however, let's simplify things for a second.

What is our definition of "**information security**"?

It doesn't get any simpler.

Information security is **risk management** related to the **confidentiality**, **integrity**, and **availability** of information.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and app oncepts

Cool!

According to the CISSP Certi tline, the subtopics are "**Confidentiality**, **integrity**, and **availability**, authenticity and nonrepudiation"

These are all VERY important; however, let's simplify things for a second.

What is our definition of "**information security**"?

It doesn't get any simpler.

Information security is **risk management** related to the **confidentiality**, **integrity**, and **availability** of information.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

According to the book, "Information security refers to the processes and methodologies involved in safeguarding information and underlying systems from inappropriate access, use, modification, or disturbance."

While this is true. Information security refers to...

The definition is, *information security **is** risk management*...

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

- **Confidentiality** – only authorized subjects should access and read information. The opposite is **disclosure**, and the risk to manage is unauthorized disclosure.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

- **Confidentiality** – only authorized subjects should access and read information. The opposite is **disclosure**, and the risk to manage is unauthorized disclosure.

Two related concepts, ***least privilege*** and ***need-to-know***.

Privacy only related to confidentiality (not integrity or availability), keeping personally identifiable information (PII) "**secret**".

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

- **Confidentiality** – only authorized subjects should access and read information. The opposite is **disclosure**, and the risk to manage is unauthorized disclosure.
- **Integrity** – ensuring that information is accurate and complete, only authorized subjects should access and change information. The opposite is **alteration**, and the risk is to manage unauthorized alteration.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept

Two related concepts, ***authenticity*** and ***nonrepudiation.***

and read information. The opposite is **disclosure**, and the risk to manage is unauthorized disclosure.

- **Integrity** – ensuring that information is accurate and complete, only authorized subjects should access and change information. The opposite is **alteration**, and the risk is to manage unauthorized alteration.

Keeping information secret is one thing, making sure it's accurate is another. Imagine if the bank didn't care about data integrity.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

- **Confidentiality** – only authorized subjects should access and read information. The opposite is **disclosure**, and the risk to manage is unauthorized disclosure.
- **Integrity** – ensuring that information is accurate and complete, only authorized subjects should access and change information. The opposite is **alteration**, and the risk is to manage unauthorized alteration.
- **Availability** – information should be available to authorized users when it's wanted/needed. The opposite is **destruction**, and the risk is to manage unauthorized destruction.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

Three availability related concepts, ***accessibility***, ***usability***, and ***timeliness.***

uthorized subjects should access
he opposite is **disclosure**, and the
thor
at in
complete, only authorized s
change information. The op
is to manage unauthorized alteration.

Obviously, information is useless when it can't be used! DDoS attacks, ransomware, etc.

- **Availability** – information should be available to authorized users when it's wanted/needed. The opposite is **destruction**, and the risk is to manage unauthorized destruction.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

The **CIA Triad** is an age-old concept.

- **Confidentiality** – only authorized subjects should access and read information. The opposite is **disclosure**, and the risk to manage is unauthorized disclosure.
- **Integrity** – ensuring that information is accurate and complete, only authorized subjects should access and change information. The opposite is **alteration**, and the risk is to manage unauthorized alteration.
- **Availability** – information should be available to authorized users when it's wanted/needed. The opposite is **destruction**, and the risk is to manage unauthorized destruction.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand a rity concepts

These must be balanced, depending on context.

The **CIA Triad** is an

- **Confidentiality** – bjects should access and read inform is **disclosure**, and the risk to manage is unauthorized disclosure.
- **Integrity** – ensuring that information is accurate and complete, only authorized subjects should access and change information. The opposite is **alteration**, and the risk is to manage unauthorized alteration.
- **Availability** – information should be available to authorized users when it's wanted/needed. The opposite is **destruction**, and the risk is to manage unauthorized destruction.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand a rity concepts

The **CIA Triad** is an

- **Confidentiality** – bjects should access and read inform is **disclosure**, and the risk to manage is unauthorized disclosure.
- **Integrity** – ensuring that information is accurate and complete, only authorized subjects should access and change information. The opposite is **alteration**, and the risk is to manage unauthorized alteration.
- **Availability** – inf available to authorized users when it's w opposite is **destruction**, and the risk is to zed destruction.

These must be balanced, depending on context.

So, the opposite of CIA is "DAD"?!

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

Variations to the **CIA Triad**.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

Variations to the **CIA Triad**.

Frankly because we **LOVE** to make things more **complicated**.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

Variations to the **CIA Triad**.

National Institute of Standards and Technology (NIST) Special Publication 800-33, "Underlying Technical Models for Information Technology Security", **added**:

- **Accountability** (that actions of an entity may be traced uniquely to that entity)
- **Assurance** (that security measures work as intended

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

Variations to the **CIA Triad**.

National Institute of Standards and Technology (NIST) Special Publication 800-33, "Underlying Technical Models for Information Technology Security", **added**:

- **Accountability** (that actions of an entity may be traced uniquely to that entity)
- **Assurance** (that security measures work as intended

Not to be outdone...

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand and apply security concepts

Variations to the **CIA Triad**.

Donn B. Parker and the **Parkerian Hexad**, added to the CIA Triad:

- **Authenticity**: The proper attribution of the person who created the information
- **Utility**: The usefulness of the information
- **Possession or control**: The physical state where the information is maintained

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

1.3 Evaluate and apply security governance principles

- Alignment of the security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks
- Due care/due diligence

This comes from the (ISC)² Certification Exam Outline

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

A definition of "security governance":

Security governance is *the set of responsibilities, policies, and procedures related to defining, managing, and overseeing security practices at an organization.*

It's always good to define what we're talking about first!

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Information security is **NOT** an IT issue. It's a business issue.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Information security is **NOT** an IT issue. It's a business issue.

This begs the question:

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Information security is **NOT** an IT issue. It's a business issue.

This begs the question:

Who is ultimately responsible for information security in a business?

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Information security is **NOT** an IT issue. It's a business issue.

This begs the question:

Who is ultimately responsible for information security in a business?

Ultimately, it's the **board of directors**. If a board doesn't exist, it's the top executive.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

A business is in business to make **money**. Or maybe to serve a **mission/purpose**.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

A business is in business to make **money**. Or maybe to serve a **mission/purpose**.

If information security does not provide value to the organization's purpose, then why are we doing what we're doing?

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

A business is in business to make **money**. Or maybe to serve a **mission/purpose**.

If information security does not provide value to the organization's purpose, then why are we doing what we're doing?

Information security **must** align with (and provide value to) the organization's mission/purpose.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

A business is in business to make **money**. Or maybe to serve a **mission/purpose**.

If i **de**
va
then why are we doing what we're doing?

Proper governance is where this starts.

Information security **must** align with (and provide value to) the organization's mission/purpose.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Applying security governance principles involves the following:

- **Aligning** information security with the company's business strategy, goals, mission, and objectives.
- Defining and managing organizational processes to **involve information security** (e.g., acquisitions, divestitures, and governance committees)
- Developing **roles and responsibilities** throughout the organization.
- Identifying one or more **security control frameworks** to align the organization with (the book says so anyway).
- Practice **due diligence and due care** always.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Aligning information security with the company's business strategy, goals, mission, and objectives.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Aligning information security with the company's business strategy, goals, mission, and objectives.

- Requires an (**intimate**) understanding of the company.
- Information security must not impede the organization's ability to operate as efficiently as possible.
- If we don't know the business mission, purpose, strategy, goals, etc., then we'd better **ask/find out**.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Defining and managing organizational processes to **involve information security** (e.g., acquisitions, divestitures, and governance committees).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Defining and managing organizational processes to **involve information security** (e.g., acquisitions, divestitures, and governance committees).

- A **governance committee** **is a group of executives/leaders** who **meet regularly** to set the direction of the company's security function and provide guidance to help the security function align with the company's overall mission and business strategy.
- The primary objective of a governance committee is to provide **oversight** for the company's security function

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Defining and managing organizational processes to **involve information security** (e.g., acquisitions, divestitures, and governance committees).

- A **governance committee** **is a group of exec**
  dire
  guid
  com
- The
  provide **oversight** for the company's security function

Information security committees are a great way to build rapport, get things approved, and assist with implementations too. **HIGHLY recommended** in practice!

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Defining and managing organizational processes to **involve information security** (e.g., acquisitions, divestitures, and governance committees).

Mergers and Acquisitions (or M&A)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Evaluate and apply security governance principles

Defining and managing organizational processes to **involve information security** (e.g., acquisitions, divestitures, and governance committees).

Mergers and Acquisitions (or M&A)

- Risks must be considered in M&A activity.
- Risks include not knowing, "buying a breach", introduction of new attack vectors, disgruntled employees, etc.
- Information security personnel should conduct a comprehensive risk assessment and conduct proper testing ahead of time.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Everyone in the organization has an information security role to play.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Everyone in the organization has an information security role to play.

This begs the question:

Does everyone know their role and the responsibilities that come with it?

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Everyone in the organization has an information security role to play.

This begs the question:

Does everyone know their role and the responsibilities that come with it?

An essential part of our job is to help define this, communicate/evangelize it, and help people fulfill their role.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (according to the book).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (according to the book).

Chief information security officer (CISO): A CISO is the **senior-level executive** within an organization who is responsible for the **overall management and supervision of the information security program**. The CISO drives the organization's security strategy and vision and is **ultimately responsible for the security of the company's systems and information**. While corporate reporting structures vary by company size and industry, most CISOs now report to a company's chief information officer (CIO) or CEO.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (reality simplified).

Chief information security officer (CISO): A CISO is the **senior-level executive** within an organization who is responsible for the **overall management and supervision of the information security program**. The CISO drives the organization's security strategy and vision and is ~~**ultimately responsible for the security of the company's systems and information**~~. While corporate reporting structures vary by cor
cor

This is **not true**, but for the exam it is. Information is an asset, and the board is "ultimately" responsible for corporate assets.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (reality simplified).

Not for the exam.

The **simplest** version of a CISO's job is just two things:

1. **Consult** the business to make good risk decisions.
2. **Implement** the business' risk decisions to the best of their ability.

organization's security strategy and vision and is ~~**ultimately responsible for the security of the company's systems and information**~~. While corporate reporting structures vary by

cor

cor

This is not true, but for the exam it is. Information is an asset, and the board is "ultimately" responsible for corporate assets.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (according to the book).

Chief security officer (CSO): A CSO is a **senior-level executive** within an organization who is generally responsible for all **physical security and personnel security**. Many organizations have merged CSO responsibilities into the CISO role, but you should be aware of the potential distinction between the two. To make matters even more confusing, some organizations refer to their overall security leader as a CSO (instead of CISO).

You should lean on context anytime you see these titles used.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (according to the book)

Exactly!

Chief security officer (CSO): A CSO is a **senior-level executive** within an organization who is generally responsible for all **physical security and personnel security**. Many organizations have merged CSO responsibilities into the CISO role, but you should be aware of the potential distinction between the two. To make matters even more **confusing**, some organizations refer to their overall security leader as a CSO (instead of CISO).

You should lean on context anytime you see these titles used.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (according to the book).

Security analyst: Someone with technical expertise in one or more security domains, performing the day-to-day work. May include things such as data analysis, firewall management, incident handling, and other operational activities.

Manager or program manager: Someone who owns one or more processes related to information security. May be the owner for compliance, vulnerability management, or any other broad set of responsibilities that are executed by security analysts.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Organizational roles and responsibilities

Common roles (according to the book).

Some general "**user**" responsibilities include the following:

- **Understand, agree, and adhere to** all:
  - relevant information security policies, procedures, standards, and guidelines.
  - relevant regulatory and compliance requirements.
  - relevant contractual obligations (such as nondisclosure agreements).
- **Complete information security training and awareness** activities by their required completion dates.
- **Report incidents** and suspected incidents according to the organization's requirements.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

(ISC)^2 defines a security control framework as:

"a notional construct outlining the organization's approach to security, including a list of specific security processes, procedures, and solutions used by the organization."

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

(ISC)^2 defines a security control framework as:

"a notional construct outlining the organization's approach to security, including a list of specific security processes, procedures, and solutions used by the organization."

Organizations often select security control frameworks based on their industry.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

(ISC)^2 defines a security control framework as:

"a notional construct outlining the organization's approach to security, including a list of specific security processes, procedures, and solutions used by the organization."

Organizations often select security control frameworks based on their industry.

There are many frameworks/standards, but we should know: **ISO/IEC 27001/2**, **NIST 800-53**, **NIST Cybersecurity Framework (CSF)**, and **CIS Critical Security Controls**.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

ISO/IEC 27001

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

ISO/IEC 27001

- Part of the ISO 27000 family of standards.
- Maintained and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- Focused on the **creation and maintenance of an information security management system (ISMS)**, describing the overall components of an ISMS.
- Most recent revision was in 2013, although its parent, ISO/IEC 27000, was revised in 2018.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

ISO/IEC 27001 - Contains 114 controls across 14 domains:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance Supplier relationships
- Information security incident management Information security aspects of business continuity management
- Compliance

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

ISO/IEC 27002

- Titled "*Security Techniques — Code of practice for information security controls*".
- More prescriptive than ISO 27001.
- Provides best- practice recommendations.

https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC standards documents are copyrighted and cannot be freely shared.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

NIST 800-53

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

NIST 800-53

- **National Institute of Standards and Technology** is a nonregulatory agency of the U.S. Department of Commerce.
- "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- Very comprehensive (and prescriptive).
- Defines hundreds of security controls across the following 18 control families.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

Freely available online.

NIST 800-53

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- Access control (AC)
- Awareness and training (AT)
- Audit and accountability (AU)
- Security assessment and authorization (CA)
- Configuration management (CM) Contingency planning (CP)
- Identification and authentication (IA) Incident response (IR)
- Maintenance (MA)
- Media protection (MP)
- Physical and environmental protection (PE) Planning (PL)
- Personnel security (PS)
- Risk assessment (RA)
- System and services acquisition (SA)
- System and communications protection (SC)
- System and information integrity (SI)
- Program management (PM)

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

NIST Cybersecurity Framework (CSF)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

NIST Cybersecurity Framework (CSF)

- First published in 2014.
- Collection of standards, guidelines, and best practices to manage cybersecurity risk.
- NIST CSF v1.1 is the current version and was released in 2018.
- In February 2013, President Obama signed executive order 13636, mandating that NIST develop an approach to combat cybersecurity risks against **critical infrastructure**.
- Consists of five core functions, each with multiple subdivisions NIST calls categories.

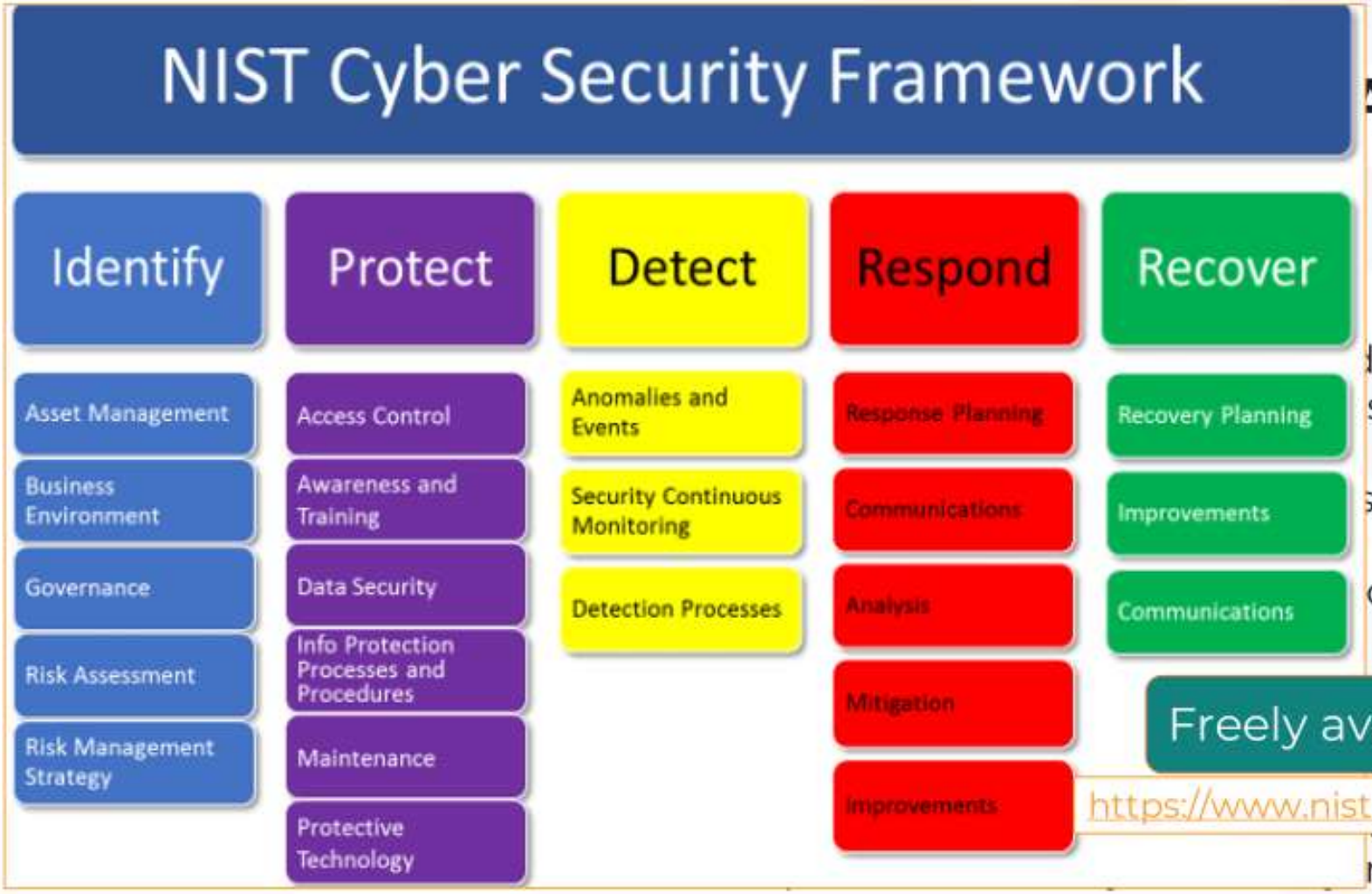
DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

NIST Cybersecurity Framework (CSF)

- NIST CSF's five **Core Functions** are:
  - **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
  - **Protect (PR)**: Develop and implement appropriate safeguards to ensure delivery of critical services.
  - **Detect (DE)**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
  - **Respond (RS)**: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
  - **Recover (RC)**: Develop and implement appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST Cyber Security Framework



AGEMENT

ding to
s, data, and
safeguards to
ctivities to
ncident.

Freely available online.

https://www.nist.gov/cyberframework

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

CIS Critical Security Controls

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

CIS Critical Security Controls

- Initially created by SANS Institute but was transferred to the Center for Internet Security (CIS) in 2015.
- CIS Controls v7.1 was released in April 2019 (20 controls)
- CIS Controls v8 was released in May 2021 (18 controls) but will most likely not be on the exam.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

CIS Critical Security Controls

- **CIS Control 1**: Inventory and Control of Hardware Assets
- **CIS Control 2**: Inventory and Control of Software Assets
- **CIS Control 3**: Continuous Vulnerability Management
- **CIS Control 4**: Controlled Use of Administrative Privileges
- **CIS Control 5**: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

All version 7.1 because this will be the version on the exam.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

CIS Critical Security Controls

- **CIS Control 6:** Maintenance, Monitoring, and Analysis of Audit Logs
- **CIS Control 7:** Email and Web Browser Protections
- **CIS Control 8:** Malware Defenses
- **CIS Control 9:** Limitation and Control of Network Ports, Protocols, and Services
- **CIS Control 10:** Data Recovery Capabilities

All version 7.1 because this will be the version on the exam.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

CIS Critical Security Controls

- **CIS Control 11:** Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
- **CIS Control 12:** Boundary Defense
- **CIS Control 13:** Data Protection
- **CIS Control 14:** Controlled Access Based on the Need to Know
- **CIS Control 15:** Wireless Access Control

All version 7.1 because this will be the version on the exam.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Security Control Frameworks

CIS Critical Security Controls

- **CIS Control 16: Account Monitoring and Control**
- **CIS Control 17**: Implement a Security Awareness and Training Program
- **CIS Control 18**: Application Software Security
- **CIS Control 19**: Incident Response and Management
- **CIS Control 20**: Penetration Tests and Red Team Exercises

CIS Critical Security Controls v8 are freely available.

https://www.cisecurity.org/controls

DOMAIN 1: SEC

Security Control
CIS Critical Security

CIS Controls Version 7	
01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8	
01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS Center for Internet Security®

https://www.cisecurity.org/controls

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Due care/due diligence

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Due care/due diligence

Very important legal terms, often used to determine negligence and liability

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Due care/due diligence

Due Care

- Refers to the **effort made** by an **ordinarily prudent** or reasonable party to avoid harm to another, taking the circumstances into account.
- The level of judgment, care, prudence, determination, and activity that a person would reasonably be expected to do under the same (or similar) circumstances.
- Regarding information security, due care relates to the conduct that a **reasonable person** would exercise to maintain the confidentiality, integrity, and availability.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Due care/due diligence

Due Diligence

- **Continually** ensuring that behavior maintains due care. In other words
- In relation to information security, due diligence relates to the ongoing actions that an organization and its personnel conduct to ensure organizational assets are reasonably protected

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Due care/due diligence

Due Diligence

- Continually ensuring that behavior maintains due care. In other words
- In relation to information security, due diligence relates to ion and its personnel ts are reasonably

Failure to demonstrate due care and/or due diligence can/will increase risk of being found negligent and/or liable for a bad event (such as a breach).

This is what "**defensible**" usually means. When a bad thing happens, is the organization "defensible" in court.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

1.4 Determine compliance and other requirements

- Contractual, legal, industry standards, and regulatory requirements
- Privacy requirements

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

Definition of "compliance"

(ISC)^2 defines compliance as:

adherence to a mandate; it includes the set of activities that an organization conducts to understand and satisfy all applicable laws, regulatory requirements, industry standards, and contractual agreements.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

Definition of "compliance"

(ISC)^2 defines compliance as:

adherence to a mandate; it includes the set of activities that an organization conducts to understand and satisfy all applicable laws, regulatory requirements, industry standards, and contractual agreements.

Contrast this with the definition of "information security" we covered earlier.

Information security is risk management.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

Legislative and Regulatory Requirements

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

Legislative and Regulatory Requirements

- The first challenge in identifying compliance requirements involves knowing **which jurisdiction has the legal authority** to set those requirements
- Jurisdiction can be determined by several different factors including (but not limited to) relevant geography or political boundaries, international treaties and agreements, activities the organization is engaged in, etc.
- Compliance is the #1 driver for information security investments.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

Legislative and Regulatory Requirements

- In most jurisdictions, laws are established to define what is permissible and what is not.
- Violations of U.S. laws may subject a party to criminal punishment or civil liability.
- Laws may be generally categorized into two parts: statutes and regulations.
  - Statutes are written and adopted by the jurisdiction's legislative body (e.g., U.S. Congress)
  - Regulations are more detailed rules on how the execution of a statute will be performed.
  - Both statutes and regulations are legally enforceable, but regulations are subordinate to statutes.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

U.S. Computer Security Act of 1987

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

U.S. Computer Security Act of 1987

- Objective of improving the security and privacy of sensitive information stored on U.S. federal government computers.
- Establishes that the **National Institute for Standards and Technology** is responsible for setting computer security standards for **unclassified**, **nonmilitary government** computer systems
- Establishes that the National Security Agency (NSA) is responsible for setting security guidance for classified government and military systems and applications
- Was repealed by the Federal Information Security Management Act (FISMA) of 2002

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Determine compliance and other requirements

U.S. Federal Information Security Management Act (FISMA) of 2002

- Requires that all U.S. federal government agencies and nongovernment organizations that provide information services to these agencies conduct risk-based security assessments that align with the NIST Risk Management Framework (RMF).
- Freely available for download: https://csrc.nist.gov/projects/risk-management/about-rmf

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

- There are **MANY**.
- The ones we're more concerned about here are:
  - U.S. Sarbanes–Oxley Act of 2002 (SOX)
  - System and Organization Controls (SOC)
  - Payment Card Industry Data Security Standard (PCI DSS)

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

U.S. Sarbanes–Oxley Act of 2002 (SOX)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

U.S. Sarbanes–Oxley Act of 2002 (SOX)

- SOX was enacted in the United States to reestablish public trust in publicly traded companies and public accounting firms following several high-profile scandals.
- Companies must implement a wide range of controls intended to **minimize conflicts of interest**, **provide investors with appropriate risk information**, place **civil and criminal penalties on executives** for providing false financial disclosures, and **provide protections for whistleblowers** who report inappropriate actions to regulators

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

U.S. Sarbanes–Oxley Act of 2002 (SOX)

- Public Company Accounting Oversight Board (PCAOB) was established as a nonprofit organization responsible for overseeing the implementation of SOX.
- PCAOB's "Auditing Standards" identify the role that information systems play in maintaining financial records and requires auditors to assess the use of IT as it relates to maintaining and preparing financial statements.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

System and Organization Controls (SOC)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

System and Organization Controls (SOC)

- Often confused with SOX
- Auditing framework that gives organizations the flexibility to be audited based on their own needs
- Three types of SOC audits and reports, **SOC 1**, **SOC 2**, and **SOC 3**.
- Audit and report types align with standards outlined in **Statement on Standards for Attestation Engagements (SSAE) 18**, published by the **American Institute of Certified Public Accountants (AICPA)** in 2017 (with amendments made via SSAE 20 in 2019).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

System and Organization Controls (SOC)

SOC 1

Audit and compliance report focusing strictly on financial statements and controls that can impact financial statements. A company that performs credit card processing may require a SOC 1 audit and compliance report.

SOC 2

Audit and compliance report that evaluates an organization based on AICPA's five "Trust Services principles": **privacy, security, availability, processing integrity,** and **confidentiality**. Many organizations undergo SOC 2 auditing and present a SOC 2 report to regulators and customers to demonstrate compliance with industry standard security controls.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

System and Organization Controls (SOC)

SOC 3

This is a "lite" version of a SOC 2 report and abstracts or removes all sensitive details. The report generally indicates whether an organization has demonstrated each of the five Trust Services principles without disclosing specifics (like exactly what they do or don't do). Companies make SOC 3 reports available to the public and restrict SOC 2 reports to trusted parties.

More information about SOC can be found on AICPA's website:
https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

Payment Card Industry Data Security Standard

https://www.pcisecuritystandards.org/pci_security/

(See the Document Library)

Version 4.0 Published March 2022

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

Payment Card Industry Data Security Standard (PCI DSS)

- Proprietary security standard established in 2004.
- Establishes technical and operational requirements for merchants and service providers (mostly).
- More than 200 security controls organized into 12 requirements, further categorized into 6 goals that generally align with security best practices.
- Not governed by or enforced by any government body.
- Compliance with PCI DSS is assessed and enforced by the payment card companies (e.g., Visa, Mastercard, American Express, etc.).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Per the PCI Security Standards Council (SSC), PCI DSS covers:

- **Build and Maintain a Secure Network**
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- **Protect Cardholder Data**
  - Requirement 3: Protect stored cardholder data.
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Per the PCI Security Standards Council (SSC), PCI DSS covers:

- **Maintain a Vulnerability Management Program**
  - Requirement 5: Use and regularly update antivirus software or programs.
  - Requirement 6: Develop and maintain secure systems and applications.
- **Implement Strong Access Control Measures**
  - Requirement 7: Restrict access to cardholder data by business need to know.
  - Requirement 8: Assign a unique ID to each person with computer access.
  - Requirement 9: Restrict physical access to cardholder data.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Industry Standards and Other Compliance Requirements

Payment Card Industry Data Security Standard (PCI DSS) 3.2.1

Per the PCI Security Standards Council (SSC), PCI DSS covers:

- **Regularly Monitor and Test Networks**
  - Requirement 10: Track and monitor all access to network resources and cardholder data.
  - Requirement 11: Regularly test security systems and processes.
- **Maintain an Information Security Policy**
  - Requirement 12: Maintain a policy that addresses information security for employees and contractors.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Privacy Requirements

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Privacy Requirements

Privacy is a subset of information security, and not the other way around.

Information security concerns itself with protecting the confidentiality, integrity, and availability of information.

Privacy concerns itself only with confidentiality of a type of information (PII).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Privacy Requirements

A CISSP® must know what PII the organization handles, and must understand the legal, contractual, and regulatory requirements that govern the privacy of that data.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

1.5 Understand legal and regulatory issues that pertain to information security in a holistic context

- Cybercrimes and data breaches
- Licensing and Intellectual Property (IP) requirements
- Import/export controls
- Transborder data flow
- Privacy

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Cybercrimes and Data Breaches

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Cybercrimes and Data Breaches

- A cybercrime is any criminal activity that directly involves computers or the internet.
- There are three major categories of cybercrimes:
  - **Crimes against people**: include cyberstalking, online harassment, identity theft, and credit card fraud.
  - **Crimes against property**: Property may include information stored on a computer, the computer itself. Includes hacking, distribution of computer viruses, computer vandalism, intellectual property (IP) theft, and copyright infringement.
  - **Crimes against government**: Cybercrime committed against a government organization is considered an attack on that nation's sovereignty. This category of cybercrime may include hacking, theft of confidential information, or cyber terrorism.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Cybercrimes and Data Br

In reality, "hacking" is not a crime. Criminal hacking is. There's a difference.

- A cybercrime is any criminal a e internet.
- There are three major categories of cybercrimes:
  - **Crimes against people**: include cyberstalking, online harassment, identity theft, and credit card fraud.
  - **Crimes against property**: Property may include information stored on a computer, the computer itself. Includes ~~hacking~~, distribution of computer viruses, computer vandalism, intellectual property (IP) theft, and copyright infringement.
  - **Crimes against government**: Cybercrime committed against a government organization is considered an attack on that nation's sovereignty. This category of cybercrime may include ~~hacking~~, theft of confidential information, or cyber terrorism.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Cybercrimes and Data Breaches

- A **data breach** a cybercrime where information is accessed or stolen without authorization. The target is the information system and the data stored within it. There are many laws that govern and regulate how cybercrimes are prevented, detected, and handled.
- CISSPs should be familiar with the some of the top/most referenced global cybercrime and information security laws and regulations.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Cybercrime

- United Nations, Cybercrime:
  https://www.unodc.org/unodc/en/cybercrime/index.html
  https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
- Interpol, Cybercrime: https://www.interpol.int/en/Crimes/Cybercrime
- Interpol, ASEAN Cyber Capacity Development Project
  https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project

https://www.interpol.int/en/content/download/16455/file/National Cybercrime Strategy Guidebook.pdf

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Interpol, National Cybercrime Strategy Guidebook (p. 10)

Table 2: Defining Cybersecurity and Cybercrime

Cybersecurity	Cybercrime
Definition	
Cybersecurity is typically defined as the protection of confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT. The concept usually covers political (national interests and security), technical and administrative dimensions.	Cybercrime is defined as offences committed against computer data, computer data storage media, computer systems, service providers. The concept usually covers categories of offences such as illegal access, interfering with data and computer systems, fraud and forgery, illegal interception of data, illegal devices, child exploitation and intellectual property infringements.

https://www.interpol.int/en/content/download/16455/file/National Cybercrime Strategy Guidebook.pdf

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

- Oldest, but still the most relevant cybercrime law currently in effect in the United States
- Has been revised over the years, amendments made in 1988, 1989, and 1999, with major amendments in 1994, 1996, and 2001 through various other acts discussed later.
- Enacted in 1986 as an amendment to the Comprehensive Crime Control Act of 1984
- Created to clarify definitions of computer fraud and abuse and to extend existing law to include intangible property such as computer data.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

- Seven criminal offenses and identifies the penalties for each:
  - **Obtaining national security information**:§1030(a) (1) describes the **felony** act of knowingly accessing a computer without or in excess of authorization, obtaining national security or foreign relations information, and willfully retaining or transmitting that information to an unauthorized party.
  - **Accessing a computer and obtaining information**:§1030(a)(2) describes the **misdemeanor** act of intentionally accessing a computer without or in excess of authorization and obtaining information from a protected computer. Upgraded to a felony if the act is committed to gain commercial advantage or private financial gain, if the act is committed in furtherance of any other criminal or tortious act, or if the value of the obtained information exceeds $5,000.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

- Seven criminal offenses and identifies the penalties for each:
  - **Trespassing in a government computer**: §1030(a)(3) extends the definition of trespassing to the computing world and describes a **misdemeanor** act of intentionally accessing a nonpublic protected computer, without authorization, and affecting the use of that computer by or for the U.S. government. §1030(a)(2) applies to many of that same cases that §1030(a)(3) could be charged, but §1030(a)(2) may be charged even when no information is obtained from the computer. In other words, section 1030(a)(3) protects against simply trespassing into a protected computer, with or without information theft.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

- Seven criminal offenses and identifies the penalties for each:
  - **Accessing to defraud and obtain value**: §1030(a)(4) was a key addition to the 1984 act, and it describes the **felony** act of knowingly accessing a protected computer without or in excess of authorization with the intent to fraud. Under §1030(a)(4), the criminal must obtain anything of value, including use of the information if its value exceeds $5,000. The key factor with §1030(a)(4) is that it allows information theft (described in §1030(a) (2)) to be prosecuted as a felony if there is evidence of fraud.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

- Seven criminal offenses and identifies the penalties for each:
  - **Damaging a computer or information**: §1030(a)(5) More generally describes a **misdemeanor** act associated with knowingly and intentionally causing damage to a computer or information. §1030(a)(5) upgrades the crime to a felony if the damage results in losses of $5,000 or more during one year, modifies medical care of a person, causes physical injury, threatens public health or safety, damages systems used for administration of justice or national security, or if the damage affects 10 or more protected computers within 1 year.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

- Seven criminal offenses and identifies the penalties for each:
  - **Trafficking in passwords**: §1030(a)(6) establishes a **misdemeanor** and prohibits a person from intentionally trafficking computer passwords or similar information when such trafficking affects interstate or foreign commerce or permits unauthorized access to computers used by or for the United States.
  - **Threatening to damage a computer**: §1030(a)(7) describes a **felony** offense associated with the computer variation of extortion. This provision prohibits threats to damage a protected computer or threats to obtain or reveal confidential information without or in excess of authorization with intent to extort money or anything else of value.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Electronic Communications Privacy Act of 1986

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Electronic Communications Privacy Act of 1986

- Enacted by the U.S. Congress in 1986 to extend restrictions on government wire taps to include computer and network- based communications (rather than just telephone calls).
- Complements the CFAA by prohibiting eavesdropping, interception, and unauthorized monitoring of all electronic communications.
- Exceptions exist to allow communications providers (like an ISP) to monitor their networks for legitimate business reasons if they first notify their users of the monitoring.
- The USA PATRIOT Act (discussed in a later section) made several extensive amendments to the ECPA in 2001.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Economic Espionage Act of 1996

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Economic Espionage Act of 1996

- Enacted by the U.S. Congress and signed into law by President Clinton in 1996.
- First federal law to broadly define and establish strict penalties for theft or unauthorized use of trade secrets.
- Criminal offense to copy, download, upload, alter, steal, or transfer trade secrets for the benefit of a foreign entity.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Child Pornography Prevention Act of 1996

- Issued in 1996 to restrict and punish the production and distribution of child pornography on the internet.

U.S. Identity Theft and Assumption Deterrence Act of 1998

- Formally established identity theft as a criminal act under U.S. federal law
- Identity theft is "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

USA PATRIOT Act of 2001

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

USA PATRIOT Act of 2001

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act
- Signed into law in 2001 in response to the terrorist attacks that took place in the United States on September 11, 2001
- Initially issued as a temporary measure, but most measures were reauthorized in 2006.
- Amends many of the provisions within the CFAA and the ECPA with new definitions of criminal offenses and new penalties.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

USA PATRIOT Act of 2001

- Section 202 — Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.
- Section 209 — Seizure of voicemail messages pursuant to warrants
- Section 210 — Scope of subpoenas for records of electronic communications
- Section 212 — Emergency disclosure of electronic communications to protect life and limb
- Section 214 — Pen register and trap and trace authority under FISA.
- Section 217 — Interception of computer trespasser communications
- Section 220 — Nationwide service of search warrants for electronic evidence

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

USA PATRIOT Act of 2001

- Section 808 — Definition of federal crime of terrorism
- Section 814 — Deterrence and prevention of cyberterrorism
- Section 815 — Additional defense to civil actions relating to preserving records in response to government requests
- Section 816 — Development and support for cybersecurity forensic capabilities

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Homeland Security Act of 2002

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Homeland Security Act of 2002

- Building off the Patriot Act's response to the September 11, 2001, terrorist attacks in the United States.
- The largest U.S. government reorganization since the creation of the Department of Defense in 1947
- With the creation of the DHS, a new cabinet-level position, Secretary of Homeland Security, was also created.
- Title X of the Homeland Security Act identifies several standards, tactics, and controls that should be used to secure U.S. federal government information.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

- Established the United States' first national standards for sending commercial emails in response to the growing number of complaints over spam (unwanted) emails.
- Requires companies to allow email recipients to unsubscribe or opt out from future emails and establishes a variety of requirements around email content and sending behavior.
- CAN-SPAM designates the Federal Trade Commission (FTC) as responsible for enforcing the provisions within the Act.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Intelligence Reform and Terrorism Prevention Act of 2004

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Intelligence Reform and Terrorism Prevention Act of 2004

- Established the National Counterterrorism Center (NCTC) and the position of the Director of National Intelligence (DNI).
- The Department of Homeland Security and other U.S. government agencies are required to share intelligence information to help prevent terrorist acts against the United States.
- Established the Privacy and Civil Liberties Oversight Board with the intent of protecting the privacy and civil liberties of U.S. citizens

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

The Council of Europe's Convention on Cybercrime of 2001

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

The Council of Europe's Convention on Cybercrime of 2001

- Also known as the Budapest Convention
- First international treaty established to address cybercrime
- Signed by more than 65 nations (the United States ratified the treaty in 2006).
- Increase cooperation among nations and establish more consistent national laws related to preventing and prosecuting cybercrime.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

The Computer Misuse Act 1990 (U.K.)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

The Computer Misuse Act 1990 (U.K.)

Introduced **five offenses** related to cybercrime:

- Unauthorized access to computer material
- Unauthorized access with intent to commit or facilitate commission of further offenses
- Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
- Unauthorized acts causing, or creating risk of, serious damage
- Making, supplying, or obtaining articles for use in other offenses

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Information Technology Act of 2000 (India)

- Amended in 2008.
- Established legal recognition of electronic documents and digital signatures, and definitions and penalties for cybercrimes such as data theft, identity theft, child pornography, and cyber terrorism.

Cybercrime Act 2001 (Australia)

- Australia's response to the September 11, 2001, terror attacks in the United States.
- Defined serious computer offenses such as unauthorized access, unauthorized modification, and unauthorized impairment of electronic communication, and established penalties for such crimes.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

- IP may include software, data, multimedia content like music and movies, algorithms, drawings, and much more.
- Several various organizations around the world that establish and protect IP rights; among them are the World Trade Organization (WTO), World Customs Organization (WCO), and the World Intellectual Property Organization (WIPO).
- Laws concerning intellectual property in the United States fit into five categories: **Licensing, Patents, Trademarks, Copyrights, Trade secrets**

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Licensing

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Licensing

- The use of unlicensed software increases the risk of software vulnerabilities, as the users are unable to get patches and updates.
- The effect of this was seen most clearly in the rapid distribution of the WannaCry malware in China, where estimates suggest that 70 percent of computer users in China are running unlicensed software, and state media acknowledged that more than 40,000 institutions were affected by the attack.
- BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Patents

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Patents

- A patent is a government-issued license or grant of property rights to an inventor that prohibits another party from making, using, importing, or selling the invention for a set period. In exchange for making the invention available to the public.
- In the United States, patents are issued by the United States Patent and Trademark Office (USPTO) and are usually **valid for 15 or 20 years**.
- Invention must be new, useful, and nonobvious.
- Patents issued by the USPTO are only valid in the United States and its territories; inventors must file patent applications in all countries where they want to be protected under national patent law.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Patents

- There is a European Patent Office (EPO), Eurasian Patent Organization (EAPO), and African Regional Intellectual Property Organization (ARIPO), among others.
- United States patent law is codified in 35 U.S.C. and 37 C.F.R. and enforced by the U.S. legal system (not the USPTO).
- A CISSP® should familiarize themselves with the patent laws in their country.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Trademarks

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Trademarks

- According to the USPTO, a trademark is "a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others."
- A service mark is a similar legal grant that identifies and distinguishes the source of a service rather than goods.

SM

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Copyrights

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Copyrights

- A copyright is a legal protection granted to the authors of "original works of authorship" that may include books, movies, songs, poetry, artistic creations, and computer software, among other categories.
- Copyrights created by an individual are protected for the **life of the author plus 70 years**.
- Original work does not need to be registered to receive copyright protections.
- Fair Use - https://www.copyright.gov/fair-use/
- 

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Trade Secrets

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Licensing and Intellectual Property (IP) requirements

Trade Secrets

- A proprietary formula, process, practice, or combination of information that a company has exclusive rights to.
- Proprietary and has economic value to the company only because of its secrecy.
- In the United States, trade secret laws are generally left up to the states, although most states have adopted the Uniform Trade Secrets Act (UTSA).

NOTE: If a trade secret isn't protected like it's a trade secret, the courts can find that it's not a trade secret.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Import/Export Controls

Especially relevant right now:

The United States, European Union, and other jurisdictions sometimes issue sanctions (government edicts that prohibit doing business with a given person, group, organization, or country) against particular countries or particular entities.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Import/Export Controls

- One of the most well-known regulations that establishes import/export controls is the U.S. International Traffic in Arms Regulations (ITAR)
- ITAR regulates the export of defense articles and defense services to keep those sensitive materials out of the hands of foreign nationals.
- ITAR applies to both government agencies and contractors or subcontractors who handle regulated materials outlined in the United States Munitions List (USML).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Import/Export Controls

- The European Union also places restrictions on dual-use technology. ECPA No. 428/2009 of May 5, 2009, requires member states to participate in the control of exports, transfer, brokering, and transit of dual-use items. In 2017, these regulations were updated to reflect controls over cyber weapons.
- Several countries have adopted laws or regulations that require security reviews to be conducted or, in some cases, denied companies the authority to import products to their countries altogether.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Privacy

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Privacy

The following regulations are **in scope** for the CISSP exam:

- U.S. Federal Privacy Act of 1974
- U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996
- U.S. Children's Online Privacy Protection Act (COPPA) of 1998
- U.S. Gramm-Leach-Bliley Act (GLBA) of 1999
- U.S. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009
- Data Protection Directive (EU) Data Protection Act 1998 (UK) Safe Harbor
  EU-US Privacy Shield
- General Data Protection Regulation (GDPR) (EU)

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Federal Privacy Act of 1974, 5 U.S.C. § 552a

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Federal Privacy Act of 1974, 5 U.S.C. § 552a

- Establishes and governs practices related to the collection, maintenance, use, and dissemination of PII by U.S. government agencies.
- Balance the government's need to maintain information about citizens and permanent residents with the rights of those individuals to keep their personal information private.

"no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Health Insurance Portability and Accountability Act of 1996 (aka HIPAA *not HIPPA*)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Health Insurance Portability and Accountability Act of 1996

- HIPAA Privacy Rule and Security Rule went into effect in 2003
- Organizations that must comply with HIPAA requirements are known as covered entities and fit into three categories:
  - **Health plans**: health insurance companies, government programs (Medicare), and military/vets' health programs that pay for healthcare.
  - **Healthcare providers**: Hospitals, doctors, nursing homes, pharmacies, and other providers that transmit health information.
  - **Healthcare clearinghouses**: Public and private organizations that process or facilitate the processing of nonstandard health information and convert it into standard data types. Usually, an intermediary between a healthcare provider and a health plan or payer of health services.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Health Insurance Portability and Accountability Act of 1996

- **HIPAA Privacy Rule** establishes minimum standards for protecting a patient's privacy and regulates the use and disclosure of individuals' health information, referred to as **protected health information (PHI)**.
- PHI is permitted to be used strictly for the purposes of performing and billing for healthcare services and must be protected against improper disclosure or use.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Health Insurance Portability and Accountability Act of 1996

- **HIPAA Security Rule** establishes minimum standards for protecting PHI that is stored or transferred in electronic form.
- Operationalizes Privacy Rule by establishing the technical, physical, and administrative controls that must be put in place to protect electronically stored PHI (or e-PHI).
- Civil penalties for HIPAA violation may include fines that range from $100 to $50,000 per violation, with a maximum penalty of $1.5 million per year for similar violations. Criminal penalties include fines up to $250,000 and potential imprisonment up to 10 years.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Health Information Technology for Economic and Clinical Health Act of 2009

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Health Information Technology for Economic and Clinical Health Act of 2009

- Referred to as the **HITECH Act**, created to promote the expanded use of electronic health records (EHRs)
- Extended HIPAA privacy protections by improving security and privacy protections for healthcare data by imposing tougher penalties for HIPAA compliance violations.
- Also introduced a new HIPAA Breach Notification Rule, covered entities are required to disclose a breach of unsecured PHI to affected parties within 60 days of breach discovery.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Children's Online Privacy Protection Act of 1998

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Children's Online Privacy Protection Act of 1998

- U.S. federal law that establishes strict guidelines for online businesses to protect privacy of children *under the age of 13.*
- COPPA applies to any organization around the world that handles the data of children residing in the United States and also applies to children that reside outside of the United States, if the company is U.S.-based.
- According to the Federal Trade Commission (FTC), civil penalties of up to $43,280 may be levied for each violation of COPPA.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Gramm-Leach-Bliley Act of 1999 (GLBA)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

U.S. Gramm-Leach-Bliley Act of 1999

- Also known as the Financial Services Modernization Act of 1999
- U.S. law that requires financial institutions to safeguard their customer's PII.
- The **Financial Privacy Rule** requires that financial institutions provide each customer with a written privacy notice that explains what personal information is collected from the customer, how it is used, and how it is protected.
- The **Safeguards Rule** requires organizations to implement proper security controls to protect their customers' personal data.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Data Protection Directive (EU)

- Officially known as Directive 95/46/EC, was enacted by the European Parliament in 1995. 1st major privacy law in the EU.
- Regulated the processing of the personal data of European citizens. Superseded by the GDPR.

Data Protection Act 1998 (UK)

- Enacts the provisions within the EU's Data Protection Directive.
- Established that UK citizens held the legal right to control their personal information
- Superseded by the Data Protection Act 2018.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Safe Harbor

- International Safe Harbor Privacy Principles, often short-handed as just "Safe Harbor".
- Agreement between the United States and European Union, established between 1998 and 2000 to reconcile differences between U.S. and EU privacy laws.
- Ruled invalid by the European Court of Justice in 2015 and replaced with the EU-US Privacy Shield soon after.

EU-US Privacy Shield

- Second attempt at above, agreement was reached in 2016
- Same court declared the EU-US Privacy Shield invalid in 2020.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU)

- Maybe the world's strongest data privacy law, established in 2016 to replace EU's 1995 Data Protection Directive.
- If an organization stores or processes personal data of EU citizens or residents, then GDPR applies, regardless of physical location.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU)

Data Controller

"The data controller determines the purposes for which and the means by which personal data is processed. So, if your company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller. Employees processing personal data within your organisation do so to fulfil your tasks as data controller." https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

Data Processor

"The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking."

European Commission

English

What is a data controller or a data processor?

PAGE CONTENTS

Answer

The **data controller** determines the **purposes** for which and the **means** by which personal data is processed. So, if your company/organisation decides 'why' and 'how' the personal data should be processed it is the data controller. Employees processing personal data within your organisation do so to fulfil your tasks as data controller.

Your company/organisation is a **joint controller** when together with one or more organisations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU)

Article 5 establishes and describes **seven principles** for processing personal data:

- **Lawfulness, fairness, and transparency**: Obtain and process personal data in accordance with applicable laws and fully inform the customer of how their data will be used.
- **Purpose limitation**: Identify "specific, explicit, and legitimate" purpose for data collection, and inform them of such purpose.
- **Data minimization**: Collect and process the minimum amount of data necessary to provide the agreed-upon services.
- **Accuracy**: Ensure that personal data remains "accurate and where necessary kept up-to-date."

https://gdpr-info.eu/ & https://eugdpr.org/

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU)

Article 5 establishes and describes **seven principles** for processing personal data:

- **Storage limitation**: Personal data may be stored only long as necessary to provide the agreed-upon services.
- **Integrity and confidentiality**: Ensure appropriate security of personal data, and provide protection against unauthorized access, and accidental loss or destruction. This includes implementing data anonymization techniques to protect your customers' identities, where necessary.
- **Accountability**: The *data controller* (i.e., the party that stores and processes the personal data) must demonstrate compliance with all principles. Many customers pursue industry-standard certifications, like ISO 27001, to demonstrate accountability and commitment to security and privacy.

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU)

Article 17 establishes a person's "**right to be forgotten**."
Grants the data subject (i.e., the person whose data is being used) the right to have their personal data deleted if one of several circumstances.

Article 25 requires "data protection by design and by default"

Article 33 establishes rules that require data controllers to notify proper authorities within 72 hours of becoming aware of a personal **data breach**.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU) - FINES

Fines are administered by individual member state supervisory authorities (83.1). Criteria are to be used to determine the amount of the:

1. **Nature of infringement**: Number of people affected, damage they suffered, duration of infringement, and purpose of processing
2. **Intention**: Whether the infringement is intentional or negligent
3. **Mitigation**: Actions taken to mitigate damage to data subjects
4. **Preventative measures**: Technical and organizational prevention.
5. **History**: Past relevant infringements, which may be interpreted to include infringements under the Data Protection Directive and not just the GDPR, and past administrative corrective actions under the GDPR, from warnings to bans on processing and fines.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

General Data Protection Regulation (EU) - FINES

Fines are administered by individual member state supervisory authorities (83.1). Criteria are to be used to determine the amount of the:

6. **Cooperation**: Cooperativeness with the supervisory authority to remedy the infringement.
7. **Data type**: Types of data the infringement impacts; see special categories of personal data
8. **Notification**: Proactively reported to the supervisory authority by the firm or a 3rd-party.
9. **Certification**: Whether the firm had qualified under-approved certifications or adhered to approved codes of conduct
10. **Other**: Other aggravating or mitigating factors, including financial impact on the firm from the infringement

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand legal and regulatory issues that pertain to information security in a holistic context

Fines can reach Up to €20 million, or 4 percent of the worldwide annual revenue of the prior financial year, whichever is higher

General D

Fines are ac

(83.1). Criter

6. **Cooperati**
   infringem
7. **Data type**: Types of data the infringement impacts, see special categories of personal data
8. **Notification**: Proactively reported to the supervisory authority by the firm or a 3rd-party.
9. **Certification**: Whether the firm had qualified under-approved certifications or adhered to approved codes of conduct
10. **Other**: Other aggravating or mitigating factors, including financial impact on the firm from the infringement

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Terms:

- **Burden of proof** - the requirement that the criminal prosecutor or civil plaintiff/claimant prove the claims they are making against the accused, or defendant.
- **Preponderance of the evidence** - used primarily in civil actions (civil suits, not civil legal system). Tipped the scales in favor of, but no "proof beyond a reasonable doubt".
- **Beyond a reasonable doubt** – used in criminal cases. The evidence must be so clear and compelling that a "reasonable" person has no doubt or reservation about the defendant's guilt after seeing it.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Administrative (investigation and NOT law)

- When discussing investigations, for $(ISC)^2$ purposes, the term administrative will refer to actions constrained to those conducted within a single organization.
- Internal investigations are typically performed when the matter involves some violation of organizational policy.
- Does not involve any external entities such as law enforcement, investors, third-party suppliers, or attackers.
- The organization can task anyone to perform investigation activities.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Administrative (investigation and NOT law)

- Burden of proof is the lowest of all investigation types.
- Management can use whatever criteria they choose to believe evidence.
- Punitive measures can include employee termination, loss of privilege, reassignment, etc.

NOTE: It's impossible to predict all the paths that an investigation may go. Care should always be taken to conduct a professional investigation. "If you're going to fast to document everything, you're going to fast.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Criminal (investigation and NOT law)

- Investigations involve prosecution under criminal laws.
- Prosecuted at the federal, state, or local level.
- Punishments can include imposing fines, imprisonment, or, in some extreme cases, even death for offenders.
- Investigations are conducted by law enforcement.

NOTE: Do not investigate criminal matters without direction from law enforcement (who has jurisdiction).
Be careful with the "color of law"!

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Civil (investigation and NOT law)

- The plaintiff in a civil case sues for compensation for a loss or relief from some type of dispute.
- The most common type of investigation that security professional are called to support (either w/plaintiff or defendant).
- The usual standard of proof is preponderance of the evidence
- If the defendant is found liable, they may be ordered to pay for damages, to stop an activity that is harming the plaintiff, or to honor a contract or agreement into which they had previously entered.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Civil (invest

- The pla
  relief fr
- The mo
  professional are called to support (either w/plaintiff or defendant).
- The usual standard of proof is preponderance of the evidence
- If the defendant is found liable, they may be ordered to pay for damages, to stop an activity that is harming the plaintiff, or to honor a contract or agreement into which they had previously entered.

The quality of your evidence is the most likely place your case will be challenged by opposing counsel.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Regulatory (investigation and NOT law)

- Involve determining whether an organization is compliant with a given regulation or legal requirement.
- Regulations have the force of law; consequently, regulatory investigations are similar to criminal investigations.
- Government agencies perform regulatory investigations to determine whether sufficient evidence exists to prove some violation of rules or regulations.
- Burden of proof for regulatory investigations is the preponderance of the evidence, and the penalties typically involve fines and injunctions.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

Industry Standards (investigation and NOT law)

- ISO/IEC 27043:2015 recommends procedural steps for conducting security incident investigations.
- ISO/IEC 27037:2012 provides guidelines for handling digital evidence.
- NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response" provides guidance to the digital forensic process.
- NIST SP 800-101 Revision 1, "Guidelines on Mobile Device Forensics"

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Information Security Governance

Security Policy and Related Documents

Organizational Policies should reflect compliance requirements.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Information Security Governance

Security Policy and Related Documents

- **Policy (Mandatory)**
  - Purpose
  - Scope
  - Responsibilities
  - Compliance
- **Policy types**
  - Program policy
  - Issue-specific policy
  - System-specific policy

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Information Security Governance

Security Policy and Related Documents

- **Policy (Mandatory)**
  - Purpose
  - Scope
  - Responsibilities
  - Compliance
- **Policy types**
  - Program policy
  - Issue-specific policy
  - System-specific policy

Contrary to popular belief, policies are not meant to be read (by everyone).

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Information Security Governance

Security Policy and Related Documents

- **Procedures**
  - Mandatory
  - Step-by-step guidance
- **Standards**
  - Mandatory
  - Specific use of a technology
- **Guidelines**
  - Recommendations; discretionary
  - Advice/advisory
- **Baselines** (or benchmarks)
  - Usually discretionary
  - Uniform methods of implementing a standard

Document	Example	Mandatory or Discretionary?
Policy	*Protect the CIA of PII by hardening the operating system*	Mandatory
Procedure	*Step 1: Install pre-hardened OS Image. Step 2: Download patches from update server. Step 3: …*	Mandatory
Standard	*Use Nexus-6 laptop hardware*	Mandatory
Guideline	*Patch installation may be automated via the use of an installer script*	Discretionary
Baselines	*Use the CIS Security Benchmarks Windows Benchmark*	Discretionary

CISSP® MENTOR PROGRAM – SESSION TWO

SESSION 2 - FIN
YOU MADE IT!

Domain 1 is a little more than ½ done.

Domain 1 can be a challenge because it's so disjointed.

Next Session - Domain 1 (part 2) - Ryan

- Policies
- Business Continuity
- Personnel
- Third-party / Supply Chain controls
- Risk Management
- Security Awareness

SESSION 2 - FIN
YOU MADE IT!

Domain 1 is a little more than ½ done.

Domain 1 can be a challenge because it's so disjointed.

Homework:

- Read up to this point or all of Domain 1.
- Take practice tests.
- Review at least two of the references we provided in this class (download for later use).
- Post at least one question/answer in the Discord Channel.