2022

Class #4 – Domain 2

Ron Woerner

Cyber-AAA Founder & CEO & vCISO
Bellevue University CyberSecurity Studies Professor

CISSP® MENTOR PROGRAM – SESSION FOUR

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials. (pdf of book)**

CISSP® MENTOR PROGRAM – SESSION FOUR

INTRODUCTION

Agenda –

- Welcome, Reminders, & Introduction
- Questions
- Domain 2 – Asset Security
  (pp. 184 pdf)

CISSP® MENTOR PROGRAM – SESSION TWO & FOUR

WHOAMI

Ron Woerner, CISSP, CISM

- Cybersecurity Professor, Bellevue University
- Chief Security Officer, Cyber-AAA

https://linktr.ee/cyberron

https://www.linkedin.com/learning/instructors/ronald-woerner?u=2189410

@ronw123

Hackers Wanted
TEDx Omaha

GETTING GOING…

Managing Risk!

Study Tips:

- Study in small amounts frequently (20-30 min)
- Flash card and practice test apps help
- Take naps after heavy topics (aka Security Models)
- Write things down, say them out loud
- Use the Slack Channels
- Exercise or get fresh air in between study sessions

Let's get going!

GETTING GOING…

Great job last week! We're through the introduction and ½ of the 1st Domain (Security and Risk Management)

- Shout Out to Ryan Cloutier for last week!

- Every week goes so fast, it's easy to forget what happened. Same for you all?
  - Everyone get some study time in?
- Check-in – Domain 1
- How many have read Domain 2?
- Questions?

CISSP® MENTOR PROGRAM – SESSION FOUR

QUESTIONS.

The most common questions:

Check your email for links

- Slack channel
  Use it for more in-depth questions / discussions
- Live session links & Recording
- Instructor slide deck
- Other Resources

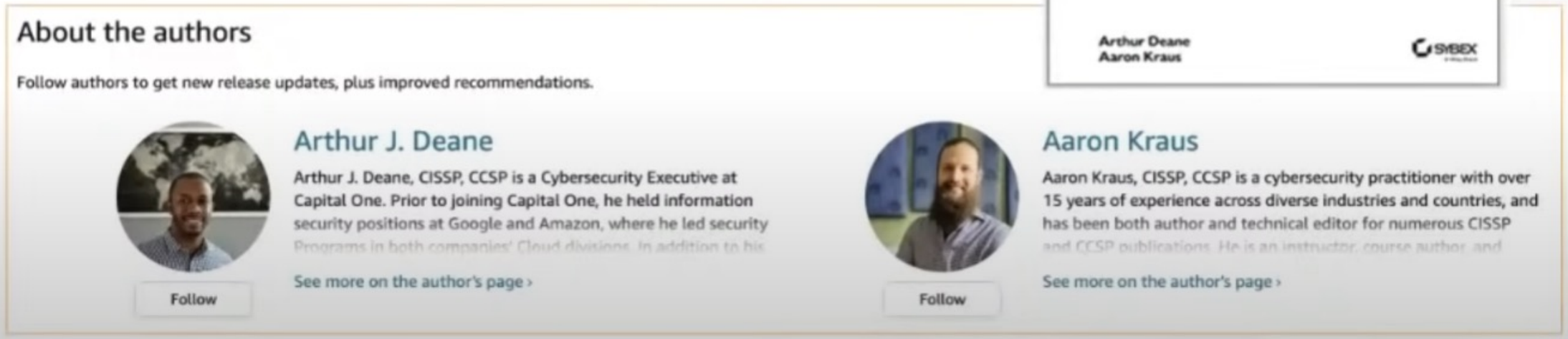
CISSP® MENTOR PROGRAM – SESSION ONE

THE BOOK

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

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

Do not share electronic versions of the book!



CISSP® MENTOR PROGRAM – SESSION FOUR

INTRODUCTION

Before we get too deep into this.

How about a dumb dad joke?

What type of bear is the most condescending?

A Pan-duh…

😂😂😂

Credit: guenterguni Getty Images

Yeah, I know.
That's dumb.

Let's get to it…

DOMAIN 1 REVIEW

You read Domain 1, right?

DOMAIN 1
Security and Risk Management

DOMAIN 1 OF THE CISSP Common Body of Knowledge (CBK) covers the foundational topics of building and managing a risk-based information security program. This domain covers a wide variety of concepts upon which the remainder of the CBK builds.

Book (pdf) pp. 31-183

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Part I Review:

- 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**

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Part 2 Review:

- Contribute to and enforce **personnel security policies and procedures**
- Identify, analyze, and prioritize **Business Continuity (BC)** requirements
- 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 FOUR

DOMAIN 1: PRACTICE QUESTION

Which of the following is not included in a standard risk assessment:

A. Identifying assets
B. Penetration test
C. Identifying threats
D. Determining risk treatment

DOMAIN 1: PRACTICE QUESTION

Which of the following is *not* included in a standard risk assessment:

A. Identifying assets
B. Penetration test
C. Identifying threats
D. Determining risk treatment

Penetration test is the least correct answer.
It's included with risk assessment & analysis.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 1: PRACTICE QUESTION

This type of document is mandatory and must be followed throughout an organization:

A. NIST Framework
B. Information Security Policy
C. Cloud benchmarks
D. WiFi Use Guidelines

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 1: PRACTICE QUESTION

This type of document is mandatory and must be followed throughout an organization:

A. NIST Framework
B. Information Security Policy
C. Cloud benchmarks
D. WiFi Use Guidelines

Policies are mandatory.
The others are discretionary.

DOMAIN 2

You read the book, right?

DOMAIN 2
Asset Security

TO APPLY AND ENFORCE effective asset security, you must concentrate on inventorying all sources of value, called *assets*. Assets can be tangible or intangible, existing in the form of information stores, databases, hardware, software, or entire networks.

Book (pdf) pp. 184-261

CISSP® MENTOR PROGRAM – SESSION TWO

DOMAIN 2: ASSET SECURITY

Topics:

If you read Domain 2 AND it felt a little disjointed, that's because it is (in the book).

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

It's okay to jump around between topics. You don't need to read the book sequentially.

← Study tip!

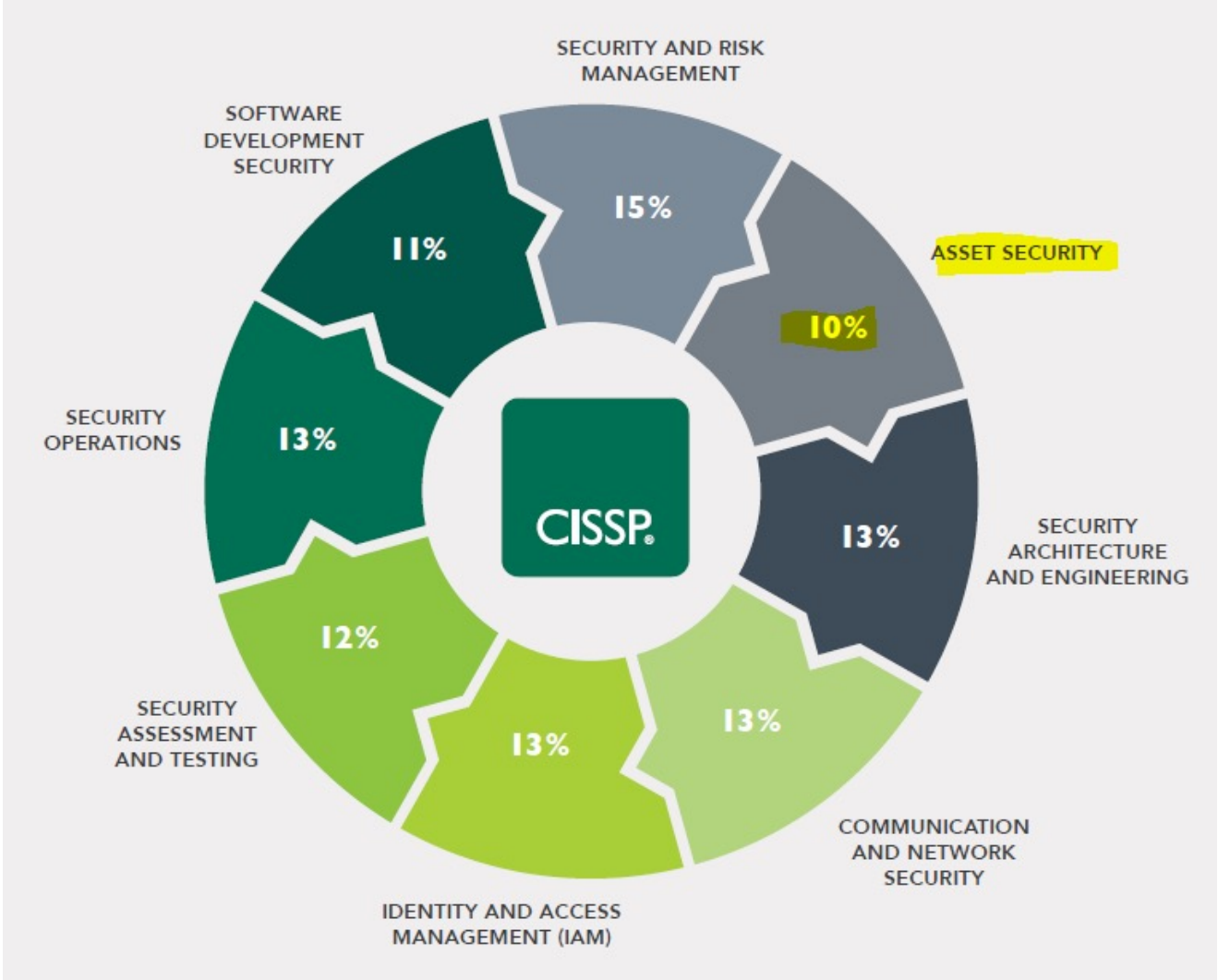
CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

CISSP Exam Overview

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

Caution!
Concepts overlap between domains.



CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

CISSP Exam Overview

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

You gotta know what you got to keep it secure…
And how important it is…

Domain 2: Asset Security

2.1 Identify and classify information and assets

- Data classification
- Asset Classification

2.2 Establish information and asset handling requirements

2.3 Provision resources securely

- Information and asset ownership
- Asset inventory (e.g., tangible, intangible)
- Asset management

2.4 Manage data lifecycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection
- Data location
- Data maintenance
- Data retention
- Data remanence
- Data destruction

2.5 Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))

2.6 Determine data security controls and compliance requirements

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Topics:

- Identify and Classify Information and Assets
- Establish Information and Asset Handling Requirements
- Provision Resources Securely
- Manage Data Lifecycle
- Ensure Appropriate Asset Retention
- Determine Data Security Controls and Compliance Requirements

pp. 184 - 261

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

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

IDENTIFY AND CLASSIFY INFORMATION AND ASSETS

Best **practices**, **policies**, and **methods** to properly **assure** the **CIA** of **organizational** information and technology **assets**.

You gotta know what you got to keep it secure…
And how important it is…

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Before I go to far, a few **supplemental references**:

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

COMPUTER SECURITY RESOURCE CENTER
CSRC

https://csrc.nist.gov/

https://www.nist.gov/cyberframework

More about this later

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Before I go to far, a couple of **supplemental references**:

https://www.cisecurity.org/

CIS Benchmarks™

Consensus-developed secure configuration guidelines for hardening.

CIS Controls®

Prescriptive, prioritized, and simplified set of cybersecurity best practices.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

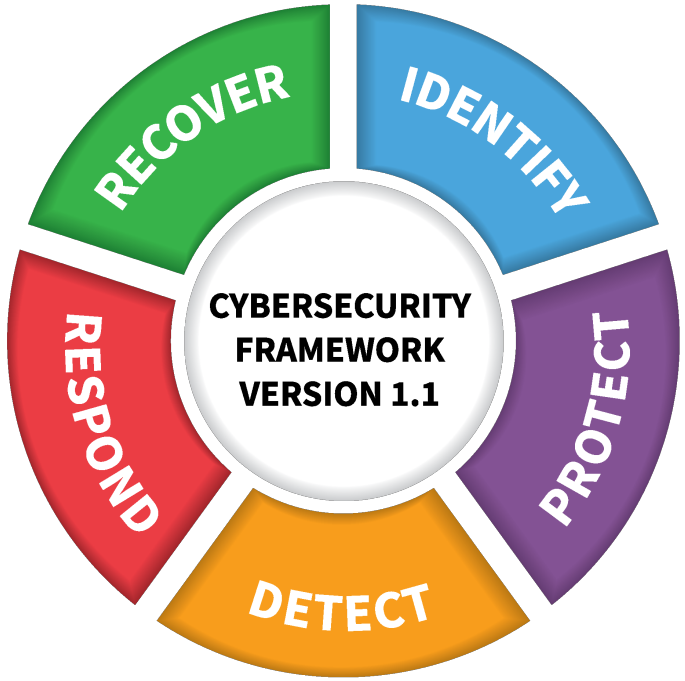
Before I go to far, a couple of **supplemental references**:

What do they have in common?

INVENTORY & ASSET MANAGEMENT

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY



Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedure		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

https://www.nist.gov/cyberframework

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

https://www.nist.gov/cyberframework

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Before I go to far, a couple of **supplemental references**:

CIS Center for Internet Security®

Confidence in the Connected World®

https://www.cisecurity.org/controls/v8/

DOMAIN 2: ASSET SECURITY

Regulations (pp. 185-186)

Canada: Security of Information Act

China: Guarding State Secrets

European Union (EU): General Data Protection Regulation (GDPR)

United Kingdom: Official Secrets Acts (OSA)

United States: NIST Federal Information Processing Standard 199, “Standards for Security Categorization of Federal Information and Information Systems”

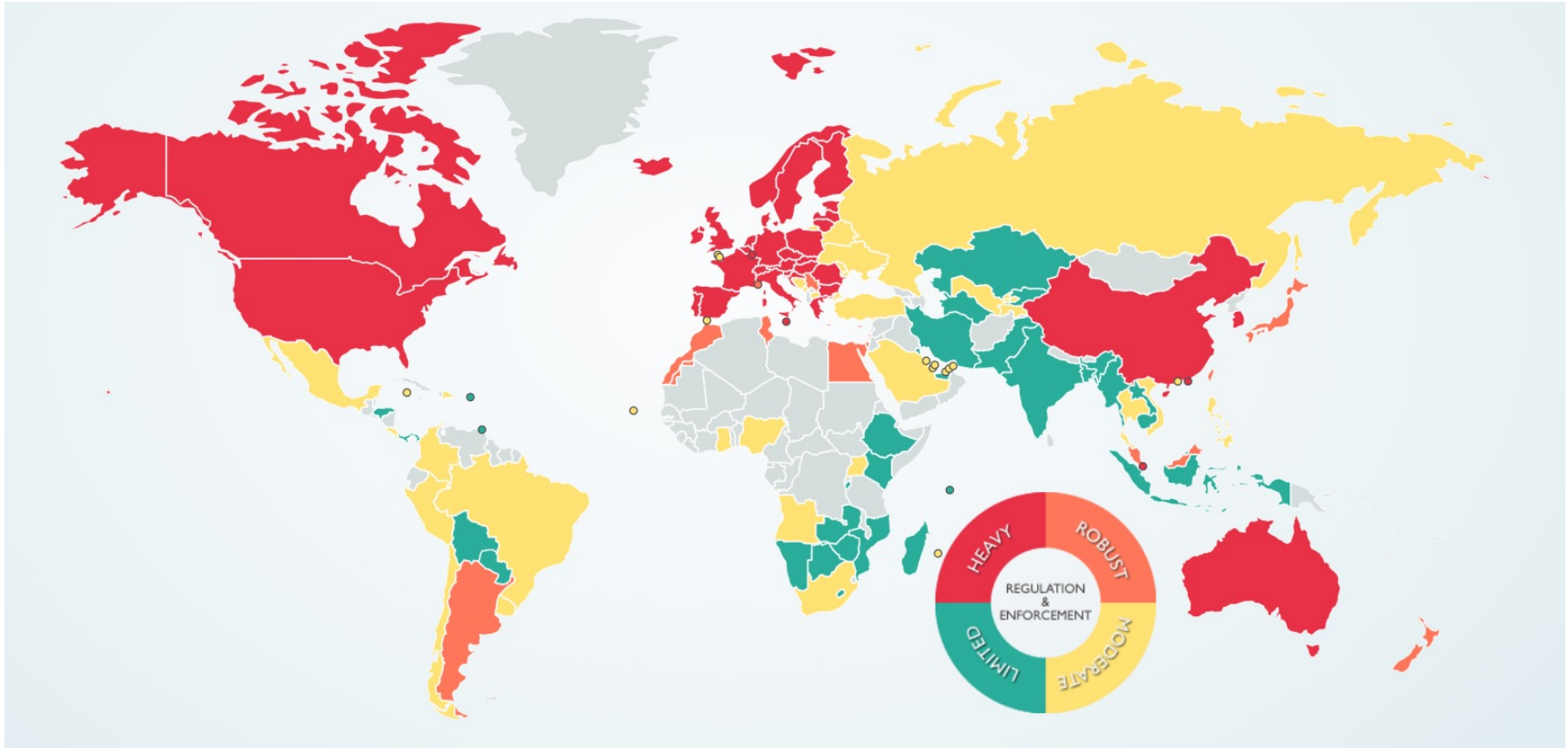
United States: NIST Special Publication (SP) 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”

United States: Committee on National Security Systems (CNSS) Instruction No. 1253, “Security Categorization and Control Selection for National Security Systems”

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Global Privacy Laws

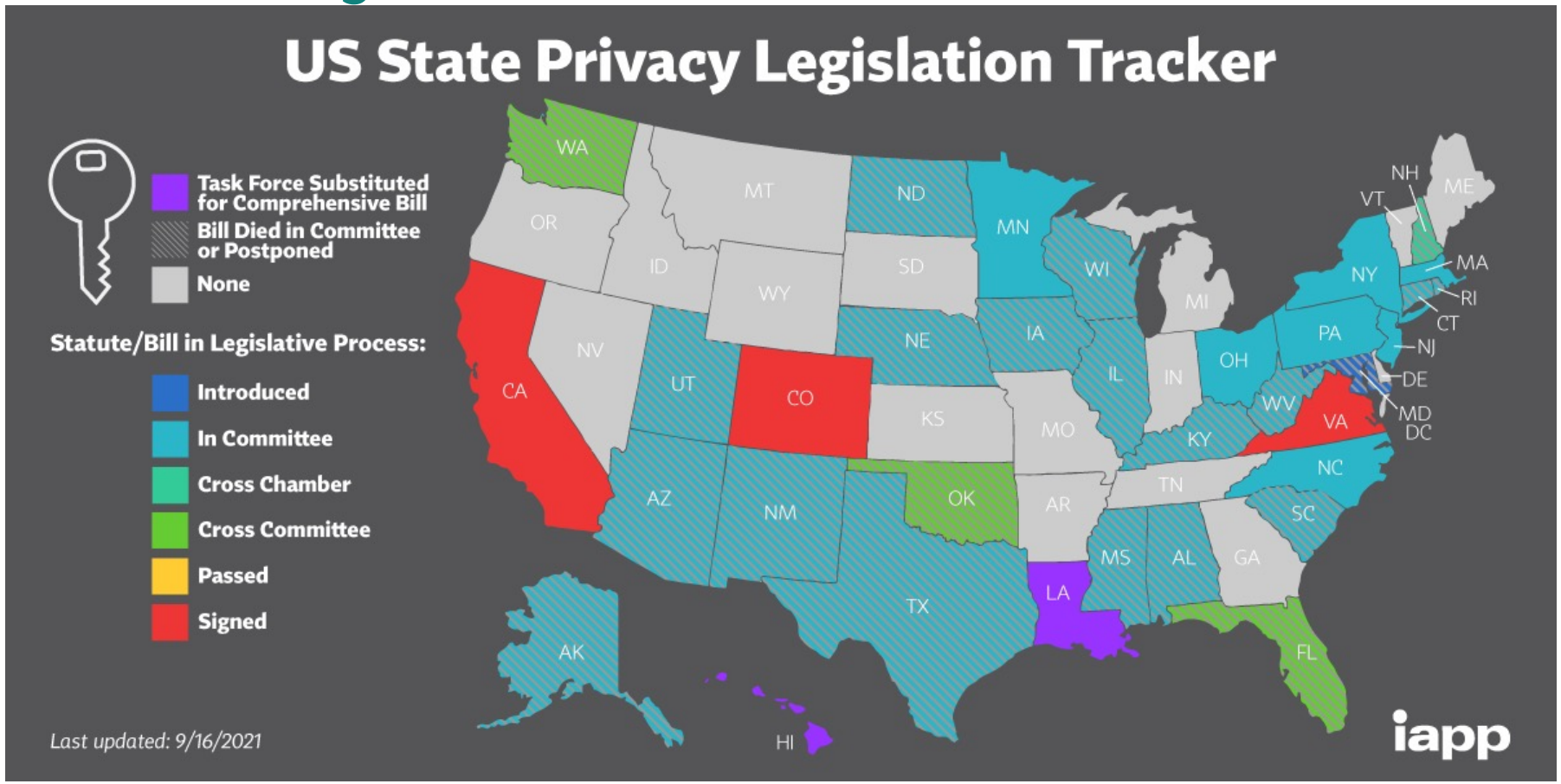


https://www.dlapiperdataprotection.com/

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

US Privacy Laws



https://iapp.org/resources/article/state-comparison-table/

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

IDENTIFY and CLASSIFY INFORMATION and ASSETS (p. 185)

- A mature security program begins with **asset identification and classification**
- Allows you to **locate** and **categorize your assets** and
- **Differentiate** the **security approaches** for each of them.
- *Having a current and complete inventory is the absolute bedrock for implementing and monitoring technical security controls*. (p.204)

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

ASSET INVENTORY

More about this later

- WHAT
  - **Hardware** (Servers, Equipment, Devices, Endpoints, etc.)
  - **Software** (Applications)
  - **Data** ← Hardest…
- WHERE
  - **Location**(s) – Physical and virtual
  - Document - **Network Diagrams** and **Data Maps**
- WHO
  - **Responsibilities** (Business & IT)

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Lifecycle (p. 214)

Before we talk about Data Classification…

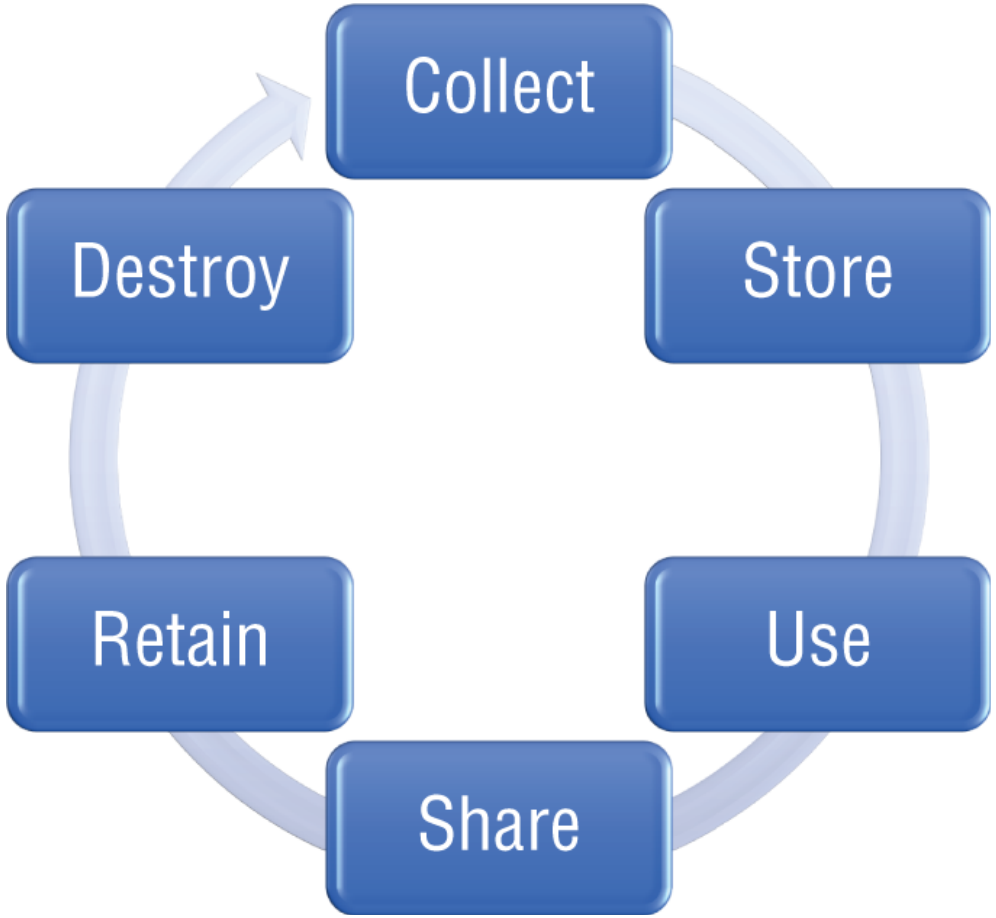


FIGURE 2.5 Secure data lifecycle

CISSP® MENTOR PROGRAM – SESSION FOUR

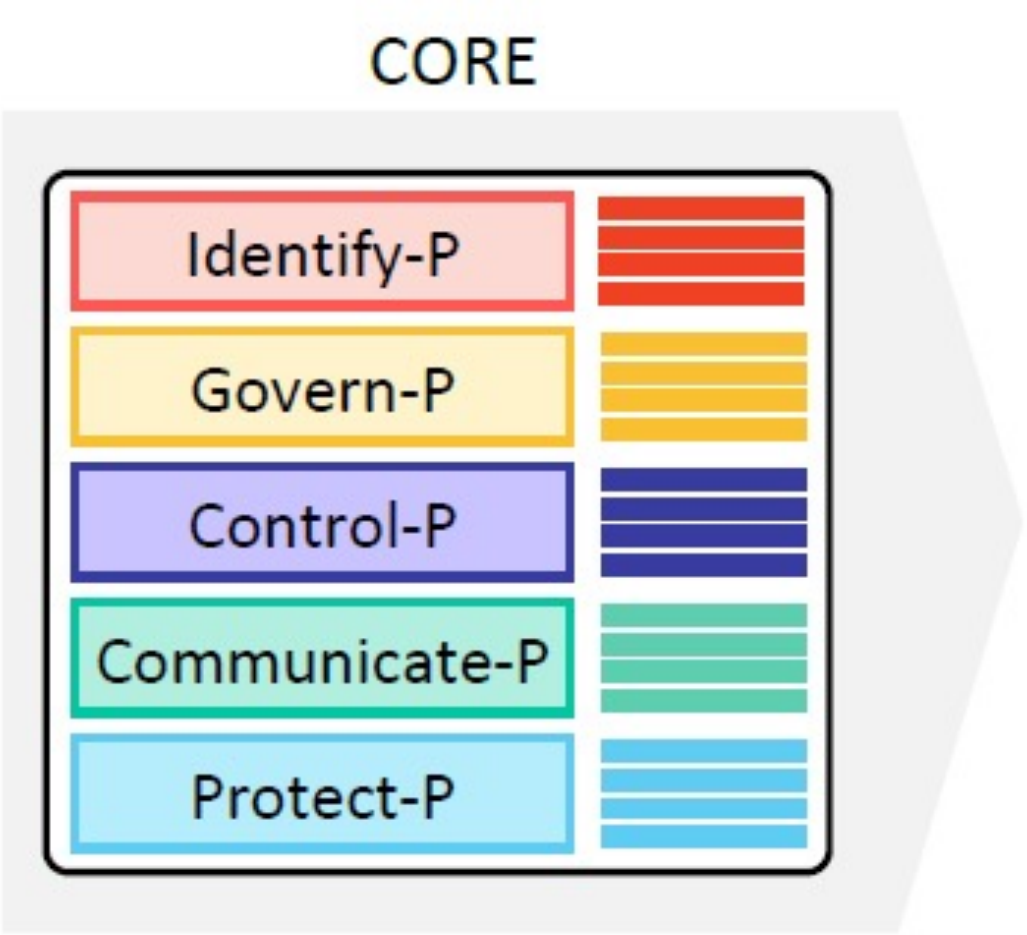
DOMAIN 2: ASSET SECURITY

Another **supplemental reference**

NIST

PRIVACY FRAMEWORK

- Privacy Framework +
- Getting Started +
- FAQs
- Resource Repository +
- Roadmap



https://www.nist.gov/privacy-framework

DOMAIN 2: ASSET SECURITY

Data Classification (pp. 186-187)

- Needed for **DATA PRIVACY**
- The **process** of **organizing data** into groups or categories that describe the data's **sensitivity, criticality, or value**.
- Determines the data's CIA Security controls.

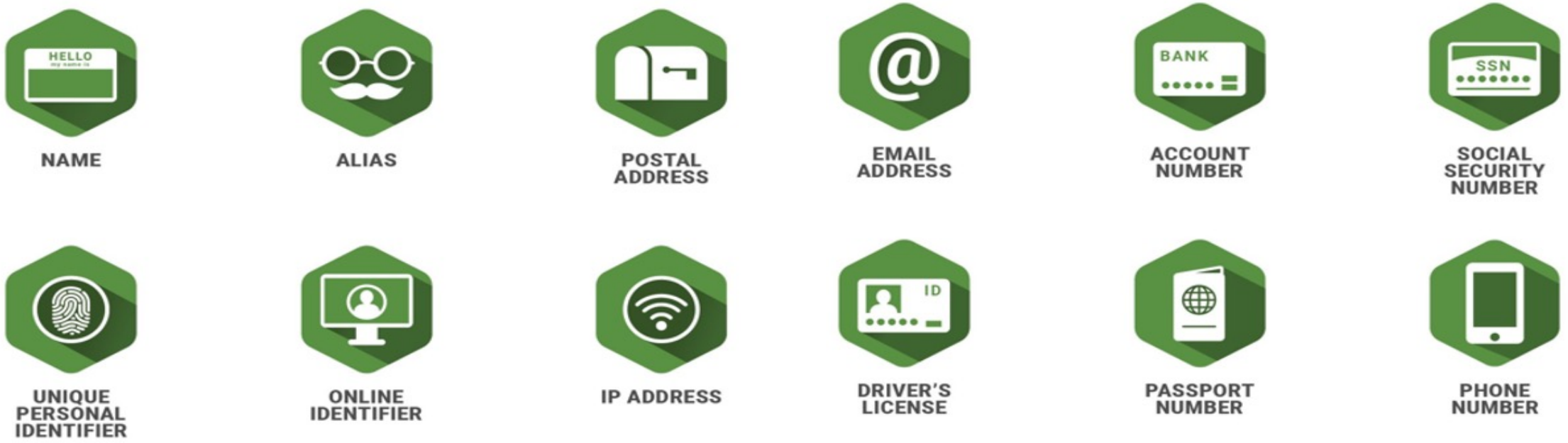
- Three Types:
  - Content-based (e.g., PII, PHI, CHD)
  - Context-based (e.g., Web browsing)
  - User-based – Manual

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Personal Information

- Who you are
- Where you are
- What you are doing



DOMAIN 2: ASSET SECURITY

Classification Schema Example (p. 188)

- Confidential
- Sensitive
- Private
- Proprietary
- Public

See the 2021 Class 3 Slides & Video

- *Many other classification are possible*
- Documented in the organization's **Data Classification Policy**
- Asset classification often based on data classification

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Classifying Data

More about this later (*Provisioning Resources*)

Formal Process for Access Approval

- Documented
- Access requests **approved by the owner**, not the manager and certainly not the custodian (more to follow).
- Approves **subject** access to certain **objects**.
- Subject must understand **rules** and **requirements** for access.
- Best practice is that all access requests and access approvals are **auditable**. [Remember – **Repudiation**]

Define Repudiation.

DOMAIN 2: ASSET SECURITY

Data Categorization (p. 189)

- The process of grouping types of data with comparable "sensitivity labels" (classifications).
- Information is categorized according to its information type.
- Apply similar security controls to assets with similar sensitivities

DOMAIN 2: ASSET SECURITY

Asset Classification (p. 190)

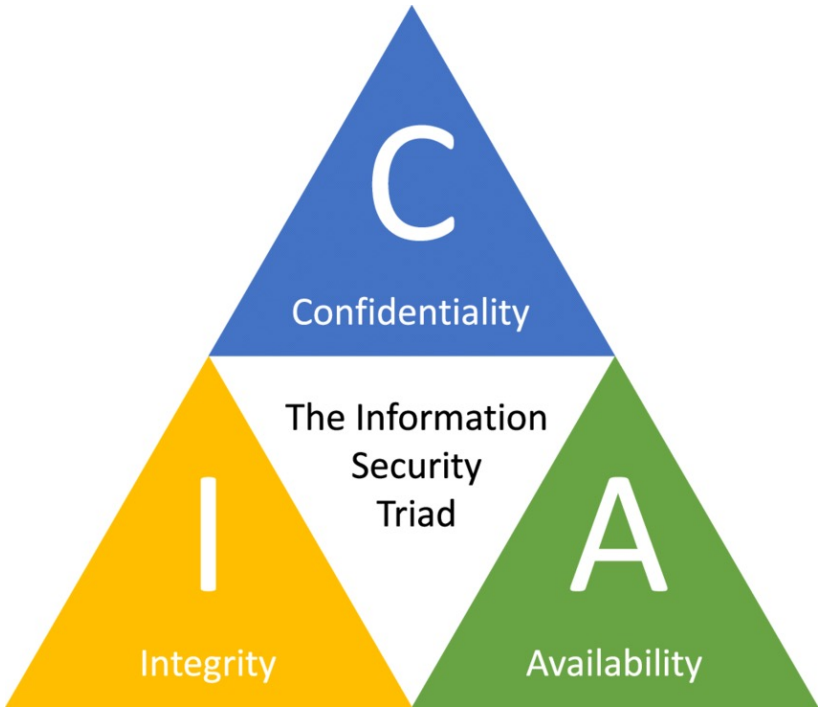
- Identifying the sensitivity, criticality, and value of information systems.
- Asset types:
  - Data
  - Hardware
  - Media (electronic & physical)
- Grouping assets based on their relative level of sensitivity and the impact to the organization should the assets be compromised.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Identify and Classify Information and Assets

Consider CIA when classifying / categorizing data and assets.



Example: Website

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Classification Benefits (p. 192)

FIGURE 2.1 General benefits of asset classification

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Asset Inventory

- Important systems, devices, software, services or data
- Tangible (hardware) and Intangible (software)
- Start with the items of highest value.

Sample Data Inventory Worksheet							
Data Type	**System**	**Environment**	**Actions**	**Data Elements**	**Owner**	**Category**	**Purpose**
PII	Personnel Database	Internal Server, HR File Share	Collect, Store	First/Last Name, SSN, Address, Phone	Human Resources	Employee	Hiring
Source: Cyber-AAA, LLC, 2022							

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

IDENTIFY AND CLASSIFY INFORMATION AND ASSETS

Best **practices**, **policies**, and **methods** to properly **assure** the **CIA** of **organizational** information and technology **assets**.

You gotta know what you got to keep it secure…
And how important it is…

Questions?
Pls put in YouTube chat or Slack.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

Which data type is *not* considered Protected or Private Information?

A. Public WiFi hotspot
B. Protected Health Information (PHI)
C. Credit Card Data
D. Website browsing and cookies

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

Which data type is *not* considered Protected or Private Information?

A. **Public WiFi hotspot**
B. Protected Health Information (PHI)
C. Credit Card Data
D. Website browsing and cookies

Because it's *Public*

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

New Topic!

ESTABLISH INFORMATION AND ASSET HANDLING REQUIREMENTS

How do you know the data or asset is important?

Marking and Labeling

Mark or label assets based on its classification.

Best practice - apply the highest level of security until the data can be determined as not sensitive

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Information and Asset Labeling & Handling

Sales Contact Details

[Your Name]

Name	Company	Work Function	Phone	Work Email	Mobile Phone	Personal Email	Address	City	ST	Zip	Notes
Jameson, Bill	ZYX Plumbing	Owner	444-555-6666	zyx@plumber.com	111-111-1111	bjames@email.com	321 Someplace Dr.	City	ST	11111	Wife has cancer
Anderson, Jane	Anon Corp	Sales Manager	222-656-7890	Janderson@anoncorp	111-111-1111						
Somers, Joe	ACME	Business Dev.	111-234-5678	jsomers@acme.com	111-111-1111	jsomers57363@gmail.com	222 First St.	City	ST	11111	Loves chocolate

Insert new rows above the gray line

AAA Cleaning - Restricted Use Only

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Information and Asset Handling – Storage

Secure Asset Storage

Physical Security

Encryption

Only store data that's needed.

Backups

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Information and Asset Handling – Declassification

- Process of **modifying** the assigned classification of an asset to a **lower level** of sensitivity.
- Used throughout the **Data Lifecycle**.
- *When / Where would you declassify data?*
- Declassification **changes security requirements**. Leads to over-securing assets.
- Manual vs. Automated.
- Part of **data governance** process. (See Domain 1)

DOMAIN 2: ASSET SECURITY

Data Declassification Methods (pp. 199-202)

Data De-identification

- Process of removing information that can be used to identify an individual.
- Quiz: *Is this used for C, I, or A (or none of the above)?* **Confidentiality**
- Takes PI data fields and converts them to **masked**, **obfuscated**, **encrypted**, or **tokenized** data fields.
- Keeps the data from being easily re-identified.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Declassification Methods (p. 201)

Data De-identification via *anonymization*

(Figure 2.2)

Gradebook

Name	Exam 1
Alice	85
Brandon	92
Cesar	79
Donna	77

Original Data

Name	Exam 1
#661243	85
#207510	92
#833384	79
#562099	77

De-identified Data

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Declassification Methods (p. 201)

Data De-identification via *masking*

(Figure 2.3)

2222 5555 6666 7890

Original Card Number

XXXX XXXX XXXX 7890

Masked Card Number

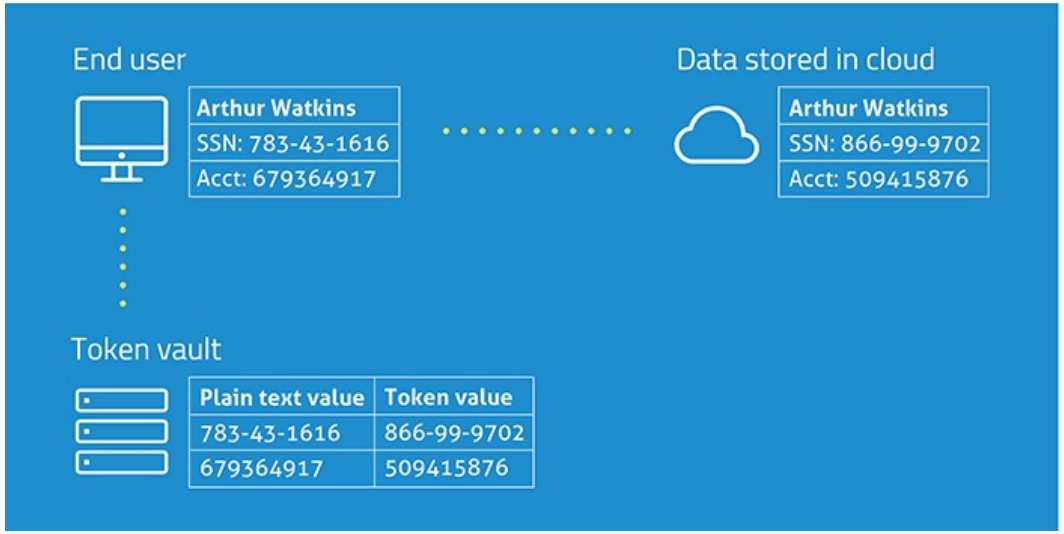
CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Declassification Methods (pp. 199-202)

Data Tokenization

- Substituting personal data with a random token
- Link between token and PI
- Random numbers or one-way functions
- Can't be reverse-engineered / deciphered



DOMAIN 2: PRACTICE QUESTION

This data de-identification technique is the process of altering personal identifiers in such a way that a data subject can no longer be identified directly or indirectly:

A. Encryption
B. Tokenization
C. Anonymization
D. Masking

DOMAIN 2: PRACTICE QUESTION

This data de-identification technique is the process of altering personal identifiers in such a way that a data subject can no longer be identified directly or indirectly:

A. Encryption

B. Tokenization

C. Anonymization

D. Masking

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

New Topic!

PROVISION RESOURCES SECURELY (pp. 202-213)

Topics:

- Information and Asset Ownership
- Asset Inventory
  - Inventory Tool / System of Record
  - Process Considerations
- Asset Management
  - Configuration Management
  - Change Management

Honestly, this domain is a little all over the place. Reminder: Jump around.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Information / Asset Ownership (pp. 202-213)

Assigning responsibility, oversight, and guidelines for asset and data management.
[Part of Governance / Policies]

Dr. Eugene Spafford's first principal of security administration:

> *If you have responsibility for security, but have no authority to set rules or punish violators, your role is to take the blame when something goes wrong.**

* Garfinkle & Spafford, *Practical Unix & Internet Security*, O'Reilly & Associates, Inc, 1996, p.39.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

New Topic!

Information / Asset Ownership (pp. 203-204)

Asset Owner Responsibilities:

- Governance / Compliance
- Asset classification
- Asset inventory
- Access oversight (Zero Trust)
- Acceptable use
- Defining, monitoring, & prioritizing safeguards (based on risk)

Lots of Responsibilities!

Rarely formalized… 😑

DOMAIN 2: ASSET SECURITY

Asset Inventory (pp. 204-207)

*Having a **current and complete inventory** is the absolute bedrock for implementing and monitoring technical security controls*. (repeated)

Inventory Tool

- System enumeration and endpoint management
- Distinguishes authorized & unauthorized assets (Shadow IT)
- Collect and track individual asset details
- For reporting, audits, risk management, and incident management

System of Record

DOMAIN 2: ASSET SECURITY

ASSET INVENTORY

Repeat Slide 32

- WHAT
  - **Hardware** (Servers, Equipment, Devices, Endpoints, etc.)
  - **Software** (Applications)
  - **Data** ← Hardest…
- WHERE
  - **Location**(s) – Physical and virtual
  - Document - **Network Diagrams** and **Data Maps**
- WHO
  - **Responsibilities** (Business & IT)

See book Pages 205-206

DOMAIN 2: ASSET SECURITY

Asset Inventory Tools

- Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) server
- Vulnerability scanners, configuration scanners, and network mapping tools (nmap)
- Software Licenses
- Data Loss Prevention (DLP)

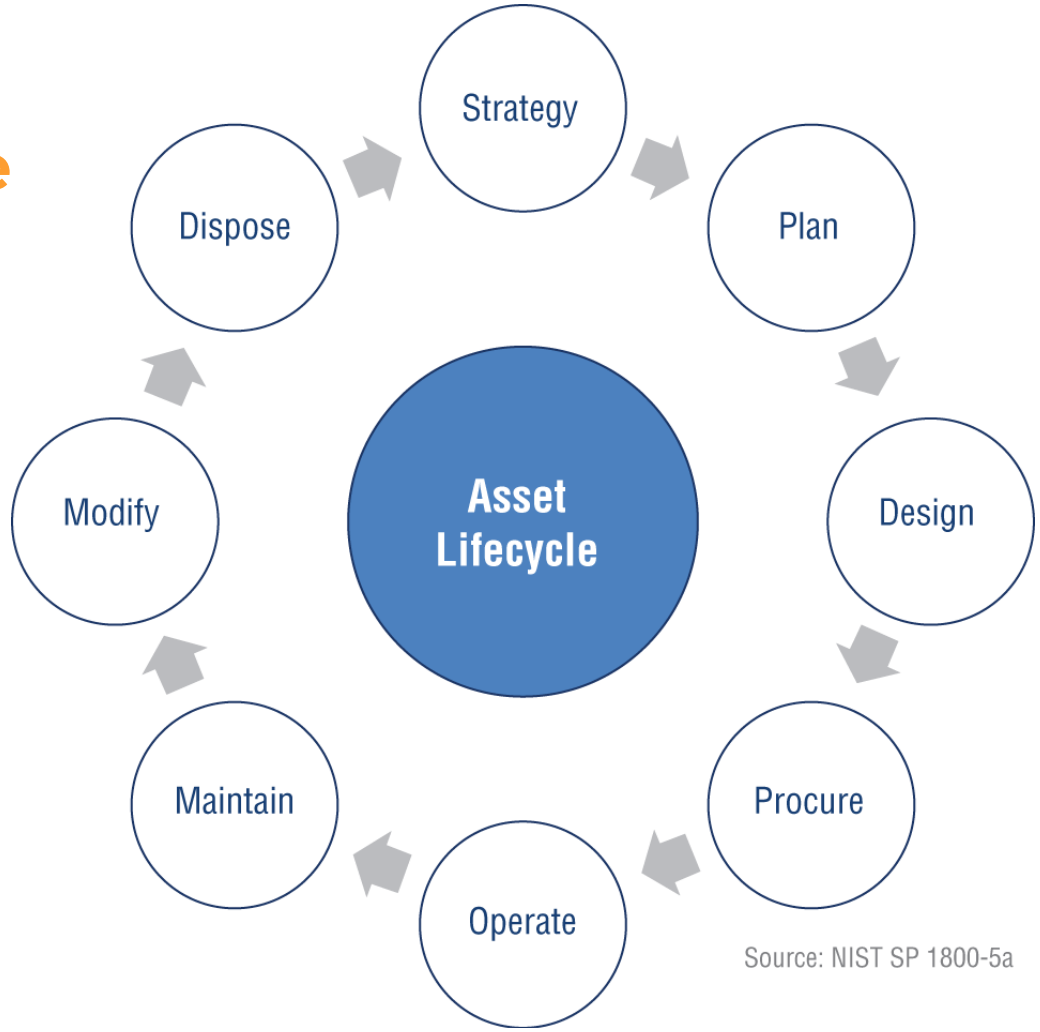
Automate as much as possible!

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Asset Management

Typical asset management lifecycle
(p. 209)



Source: NIST SP 1800-5a

Questions?
Pls put in YouTube chat or Slack.

DOMAIN 2: ASSET SECURITY

Implementing Asset Management

Information Technology Asset Management (ITAM)

- Tracking and efficiently using tangible and intangible IT Assets

ISO/IEC 19770 Family (p. 211)

- Assist organizations with managing risks and costs associated with IT assets

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

More in Domain 7

Implementing Asset Management

Configuration Management

- Maintaining asset inventory by controlling system and software configurations
- Configuration Management Database (CMDB)

Baselines

- System – product versions & settings
- Security – patches

NIST SP800-70 [National Checklist Program (NCP)]

Security Content Automation Protocol (SCAP)

Automate as much as possible!

DOMAIN 2: ASSET SECURITY

More in Domain 7

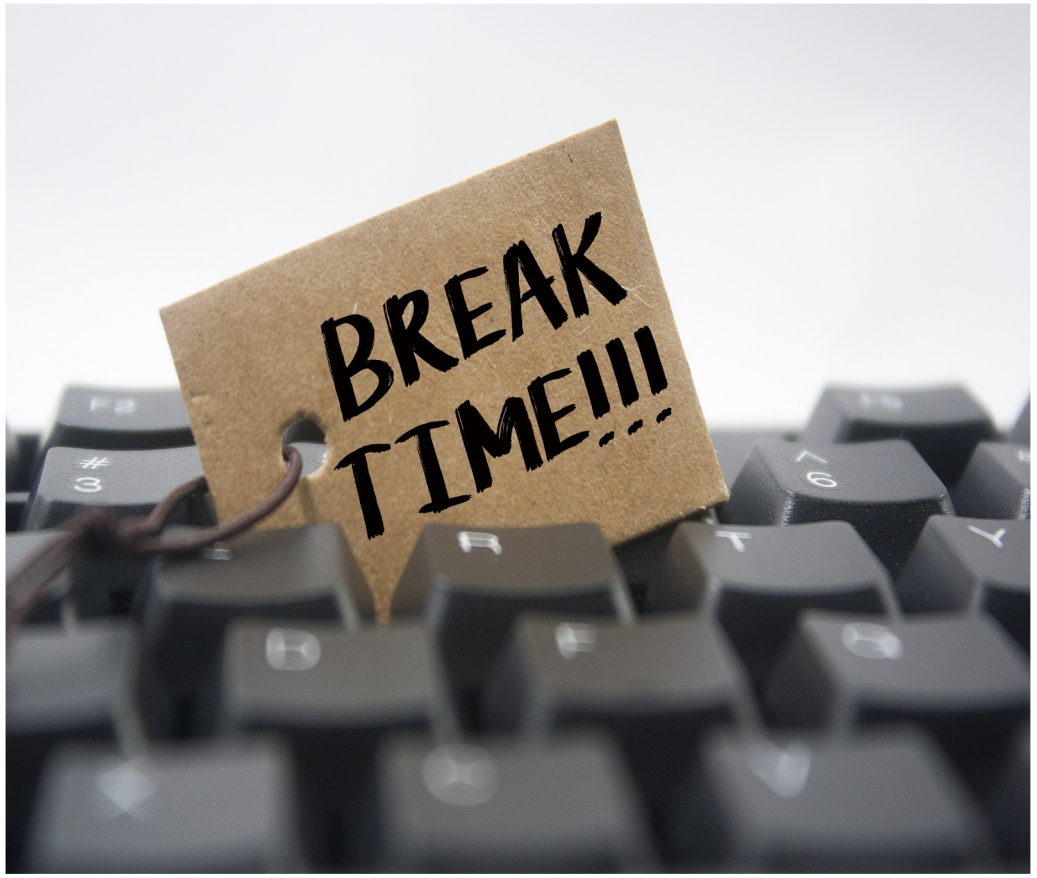
Implementing Asset Management

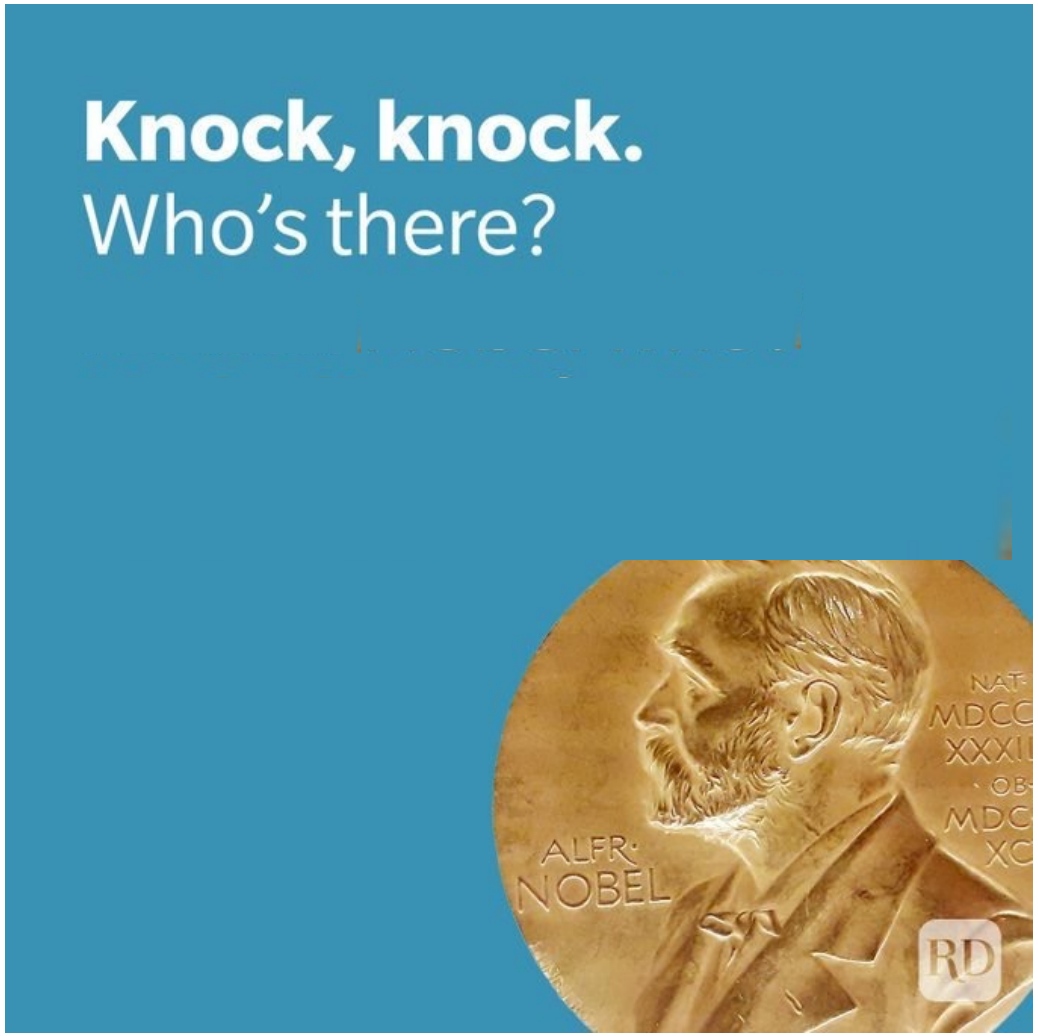
Change Management (p. 213)

- Ensuring that organizations employ standardized processes to make changes to their assets
- Standard change control processes and oversight. Change:
  - Authorization
  - Enforcement
  - Verification
- Documented (Ticketing system & CMDB)

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY





CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

New Topic!

MANAGE *DATA* LIFECYCLE (pp. 213-232)

Topics:

- Data Roles
  - Owners
  - Controllers
  - Custodians
  - Processors
  - Users
  - Subjects
- Data Collection
- Data Location
- Data Maintenance
- Data Retention
- Data Destruction
- Data Remanence

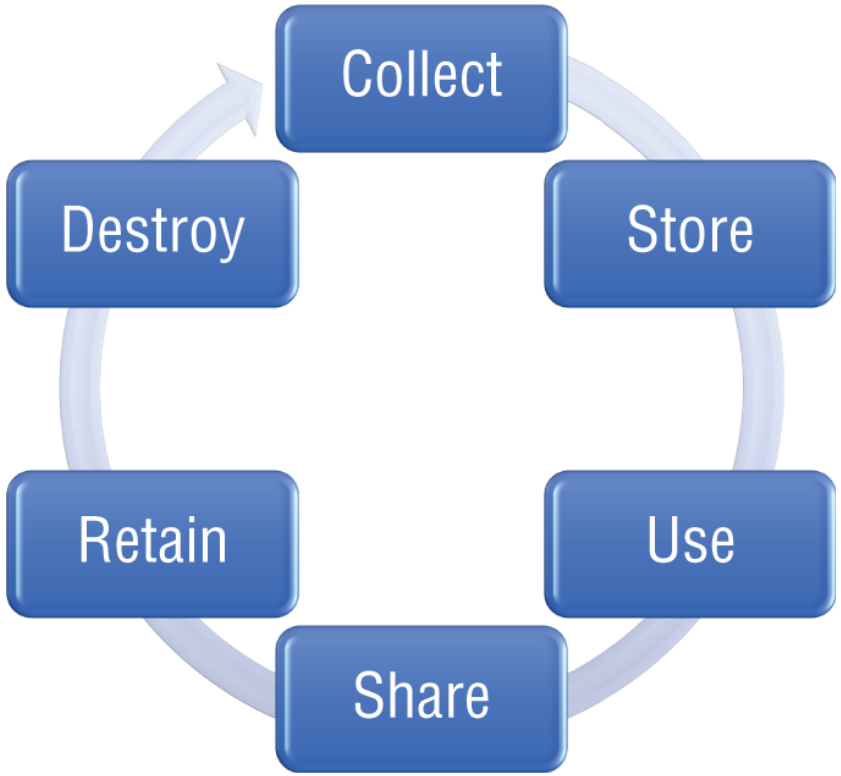


FIGURE 2.5 Secure data lifecycle

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Lifecycle (p. 214)

Review

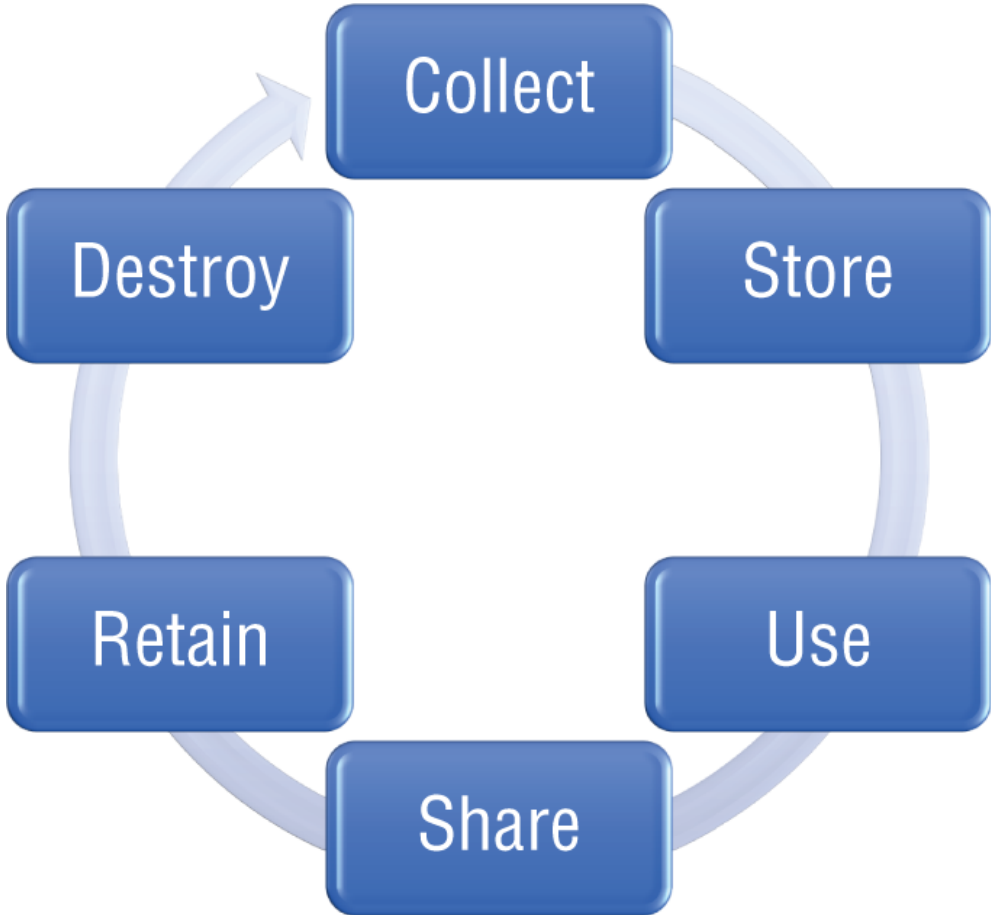


FIGURE 2.5 Secure data lifecycle

DOMAIN 2: ASSET SECURITY

Data Oversight Roles

Due Care
Due Diligence

Data Owner (p. 215)

- An individual or group of individuals responsible for dictating how and why data should be used;
- Determines how the data must be secured (risk treatment);
- Knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed;
- Determines the appropriate value and classification of information generated by the owner or department;
- Communicates Data Classification.

DOMAIN 2: ASSET SECURITY

Data Oversight Roles

Data Controller (p. 215)

- The person, agency, company, or other body that, alone or jointly with others, determines the purposes and means of data processing.
- Responsible for adhering to all principles relating to processing personal data.
- Negotiate privacy protections / *data processing agreements*
- EU GDPR

DOMAIN 2: ASSET SECURITY

Data Oversight Roles

Data Custodians (p. 218)

- Maintains the protection of data according to the information classification.
- Delegated by the Data Owner and is usually IT personnel.

Data Processors (p. 219)

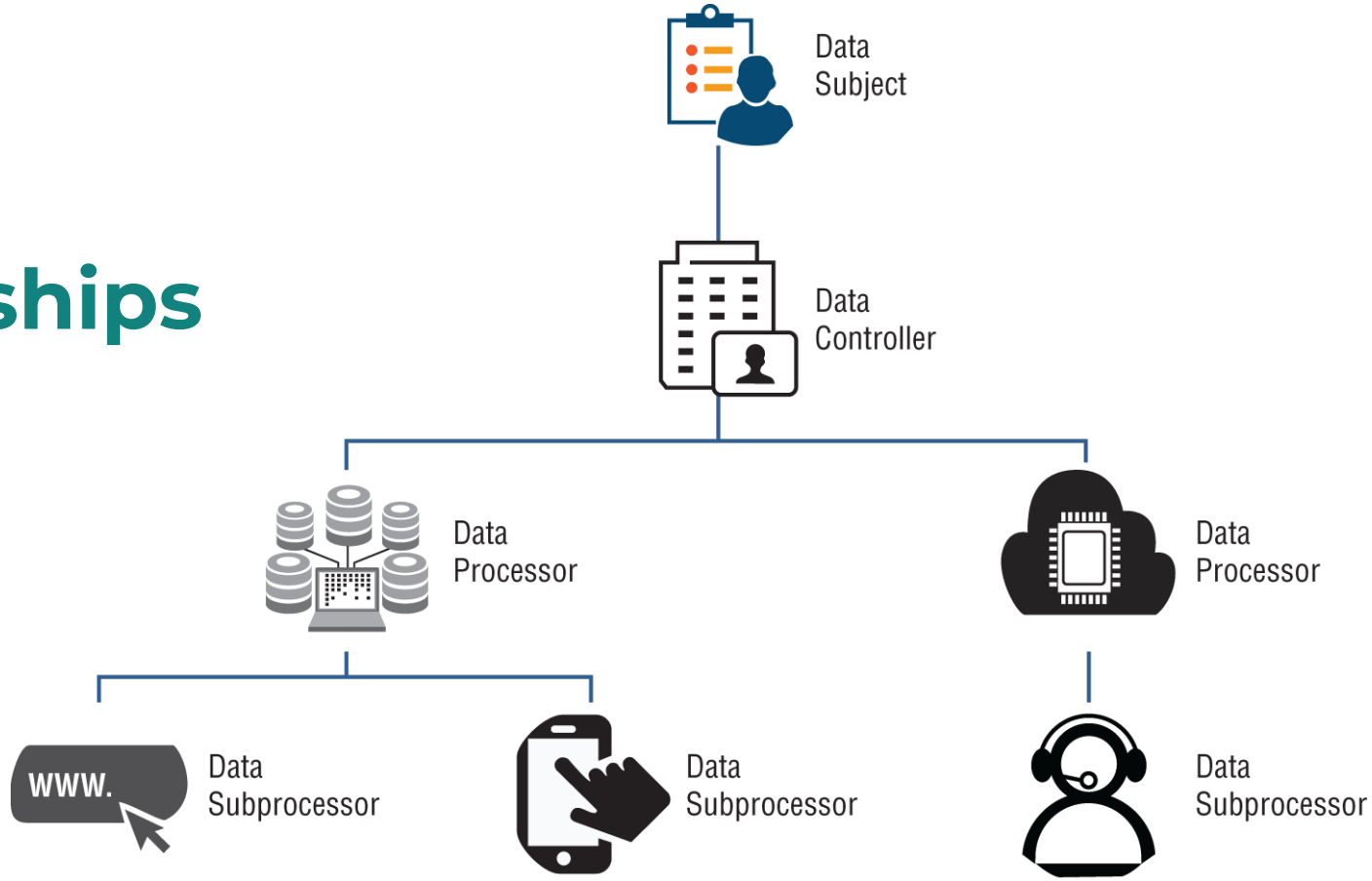
- The party responsible for transferring, transmitting, or otherwise handling data on behalf of a *data owner*.
- Role in the protection of data.
- Examples: Healthcare, Banking, Credit Processing

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data
Oversight
Roles / Relationships

Figure 2.6
p. 220



- *Data controller determines the need and how the data will be processed.*
- *Data processor is a separate legal entity processing data for the controller.*
  - *Cloud providers are generally considered data processors, as are market research firms, payroll companies, accountants.*

DOMAIN 2: ASSET SECURITY

Data Oversight Roles

Know the Difference

Data Users

- Party that consumes the data.
- May hold data processors accountable for SLAs and protection.

Data Subjects

- Defined by GDPR, are “identified or identifiable natural people” — or just human beings,
- From whom or about whom information is collected

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

This role maintains the protection of data according to the information classification:

A. Data Protection Officer
B. Data Owner
C. Data Controller
D. Data Custodian

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

This role maintains the protection of data according to the information classification:

A. Data Protection Officer

B. Data Owner

C. Data Controller

D. Data Custodian

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

Which of the following describes a duty of the Data Owner:

A. Patch systems
B. Report suspicious activity
C. Ensure their files are backed up
D. Ensure data has proper security labels

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

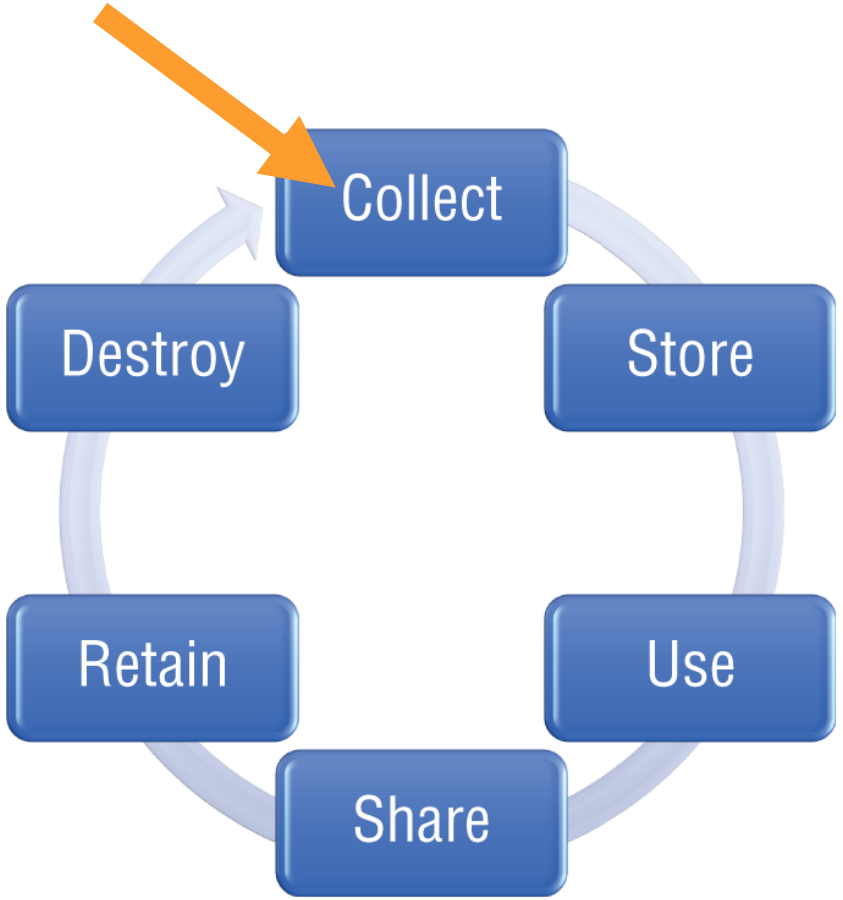
Which of the following describes a duty of the Data Owner:

A. Patch systems
B. Report suspicious activity
C. Ensure their files are backed up
D. Ensure data has proper security labels

DOMAIN 2: ASSET SECURITY

Data Collection (p. 221)

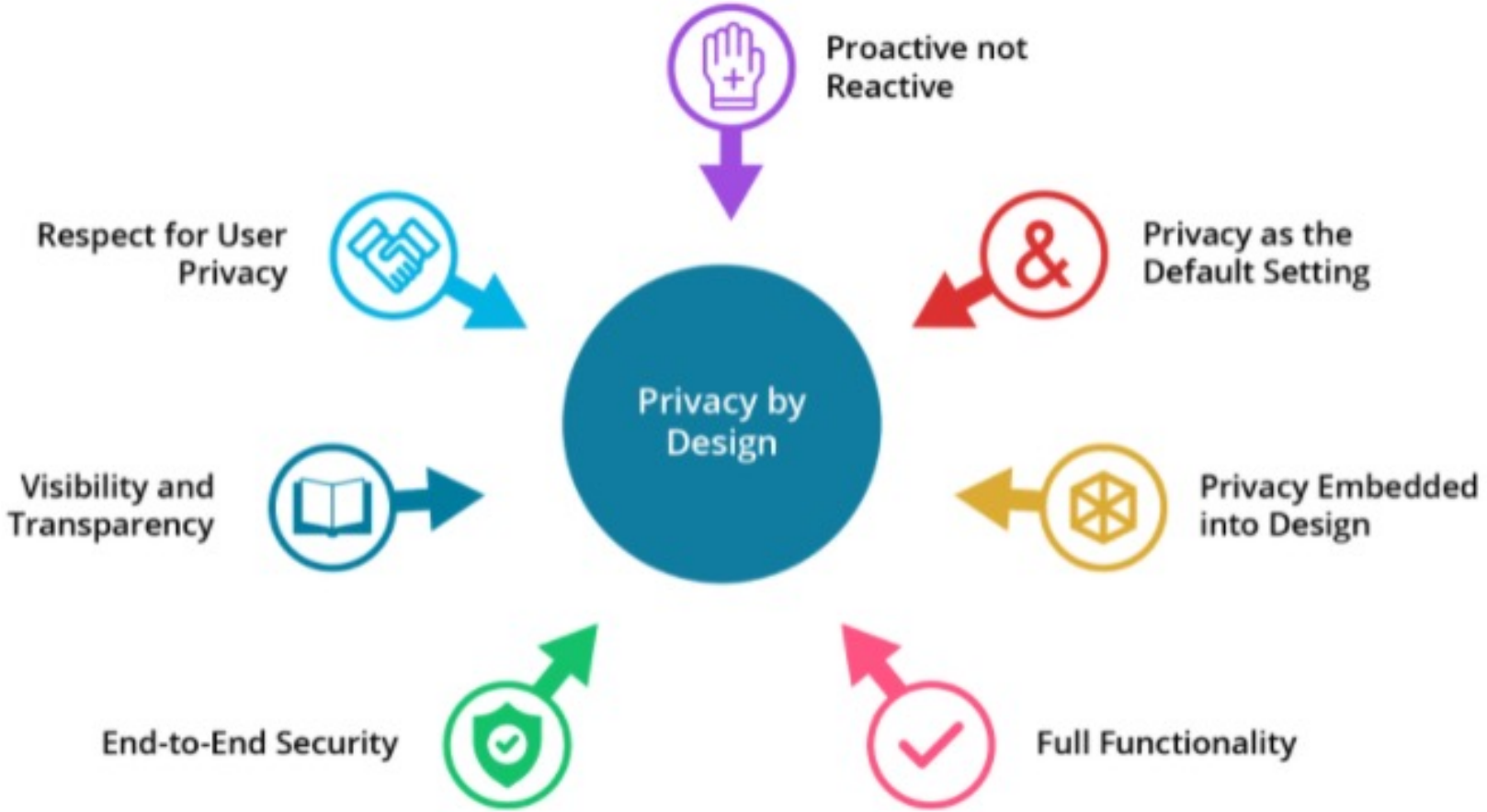
- Data creation, acquisition, aggregation, or any circumstance where data is “new” to your system
- Build Security / Privacy In …
- Organizations should **collect the minimum amount of sensitive information necessary**;
- Collection Limitation Principle – GDPR Individual Rights



CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Privacy by Design – 7 Foundational Principles



Source: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Privacy by Design – 7 Foundational Principles

Principle	Case Study Use
Proactive not Reactive	Clear executive commitment / Enforce standards Threat modeling
Privacy as the Default Setting	Explicitly state purpose of data use Collection limitation
Privacy Embedded into Design	Protected data stores
Full Functionality	Includes usability, functionality, quality, security and privacy
End-to-End Security	Full data protect through its lifecycle
Visibility and Transparency	Operating according to policies Establish trust
Respect for User Privacy	Keep systems and operations user-centric
Zero Trust	Access Controls: Network, Systems, Applications, & Data

Source: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Management

Privacy Principles

Data Use / Purpose

- Why is the data collected? (Documenting data purpose)
- User notification of intent.

Data Location

- Where is the data? (Physical & Logical)
- Data Localization

Questions?
Pls put in YouTube chat or Slack.

DOMAIN 2: ASSET SECURITY

Data Management

Data Maintenance

- Applying appropriate security controls through the “use” phase
- Balance between functionality and security
- Part of *Zero Trust* principles (Least Privilege and Defense in Depth)

Data Retention

- Time period for keeping data before destruction
- Determined by policy (often legal)

TIP The less data you have, the less damaging a security breach will be.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

TIP: *If you don't need data, securely destroy it.*

Data Management

Data Destruction / Remanence

- Logically or physically destroying unneeded data, you can both reduce your risk exposure and decrease your storage and data maintenance costs.
- Data that is left over is called ***remnant data*** - occurs when data destruction efforts were insufficient to prevent the reconstruction of the data.
- Deleting data and/or formatting a hard drive is not a viable/secure method for destroying sensitive information.
- Residual data and temporary files (cache) can remain on media.

ISSUE: Cloud Service Providers

Certificate of Destruction

DOMAIN 2: ASSET SECURITY

Data Management

Data Destruction Regulations & Frameworks

US

- GLBA
- HIPAA
- Fair Credit Reporting

European standard BS EN 15713, “Secure Destruction of Confidential Information”

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

See the 2021 Class 3 Slides & Video

Data Management

Data Destruction Methods (p. 225-232)

Often determined by law

Methods:

1. Render the object useless
   - Destruction (Physical) – Shredding, Incineration, Disintegration
2. Cleansing / Sanitizing
   - Overwriting / Clearing / Zeroing
   - Degaussing / Purging
   - Destroying encryption keys

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

New Topic!

ENSURE ASSET RETENTION (pp. 232-239)

Topics:

- Determining Appropriate Records Retention
- Records Retention Best Practices

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

ENSURE ASSET RETENTION

Why Retention:

- Preserve Intellectual Property (IP)
- Support institutional memory
- Legal / Regulatory requirements
- Evidence of actions
- Forensics investigations

You answer first… Why do organizations need to retain data?

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data / Asset Retention

Data Retention Policy

Book intermingles data and asset retention…

Don’t forget IT audit logs!

Part of Data Protection Policy

- Assign Responsibility: Data Protection Officer (DPO) and/or Chief Security Officer (CSO)
- See p. 234 for more on building a Data Use Policy
- Appropriately manages and protects data & assets throughout the lifecycle.
- Data should be assigned a retention limit based on regulatory / organizational requirements.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data / Asset Retention

Determining Appropriate Records Retention (p. 235-237)

- EU GDPR's Article 17, "*The Right to Erasure*," commonly called the *right to be forgotten*.
- Organizations need procedures to erase data.
- Note exceptions
- Consult legal

Originally from 1890's Louis Brandeis...

DOMAIN 2: ASSET SECURITY

Consult Legal

Data / Asset Retention

Records Retention Best Practices (p. 237-239)

- Handle and retain records in accordance with applicable laws, directives, policies, regulations, standards, and operational requirements.
- Maintain records according to the organization's record retention schedule.
- *Don't keep it if you don't need it.*
- Contained in the **Data Protection / Retention Policy & Procedures**.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

New Topic!

DETERMINE DATA SECURITY CONTROLS AND COMPLIANCE REQUIREMENTS (pp. 239-259)

Topics:

- Data States
  - Data at Rest
  - Data in Motion
  - Data in Use
- Scoping and Tailoring
  - Common Controls
  - Compensating Security Controls
- Standards Selection
  - Leading Security Frameworks
  - Security Standards
- Data Protection Methods
  - Digital Rights Management
  - Data Loss Prevention (DLP)
  - Cloud Access Security Broker

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

People, Process, & Technology

Data Security Controls

Control Types (p. 240 & 247)

- Security controls will vary based on the classification of each asset, the data state (discussed next), and any compliance requirements or industry standards.
- Technical Controls
- Administrative Controls
- Physical Controls

P. 247 – Common Controls

> **NOTE** When thinking of the three types of controls, remember that technical controls shape the behavior of hardware and software, administrative controls shape the behavior of humans, and physical controls shape the behavior of anything that moves (which may include humans, robots, IoT devices, etc.).

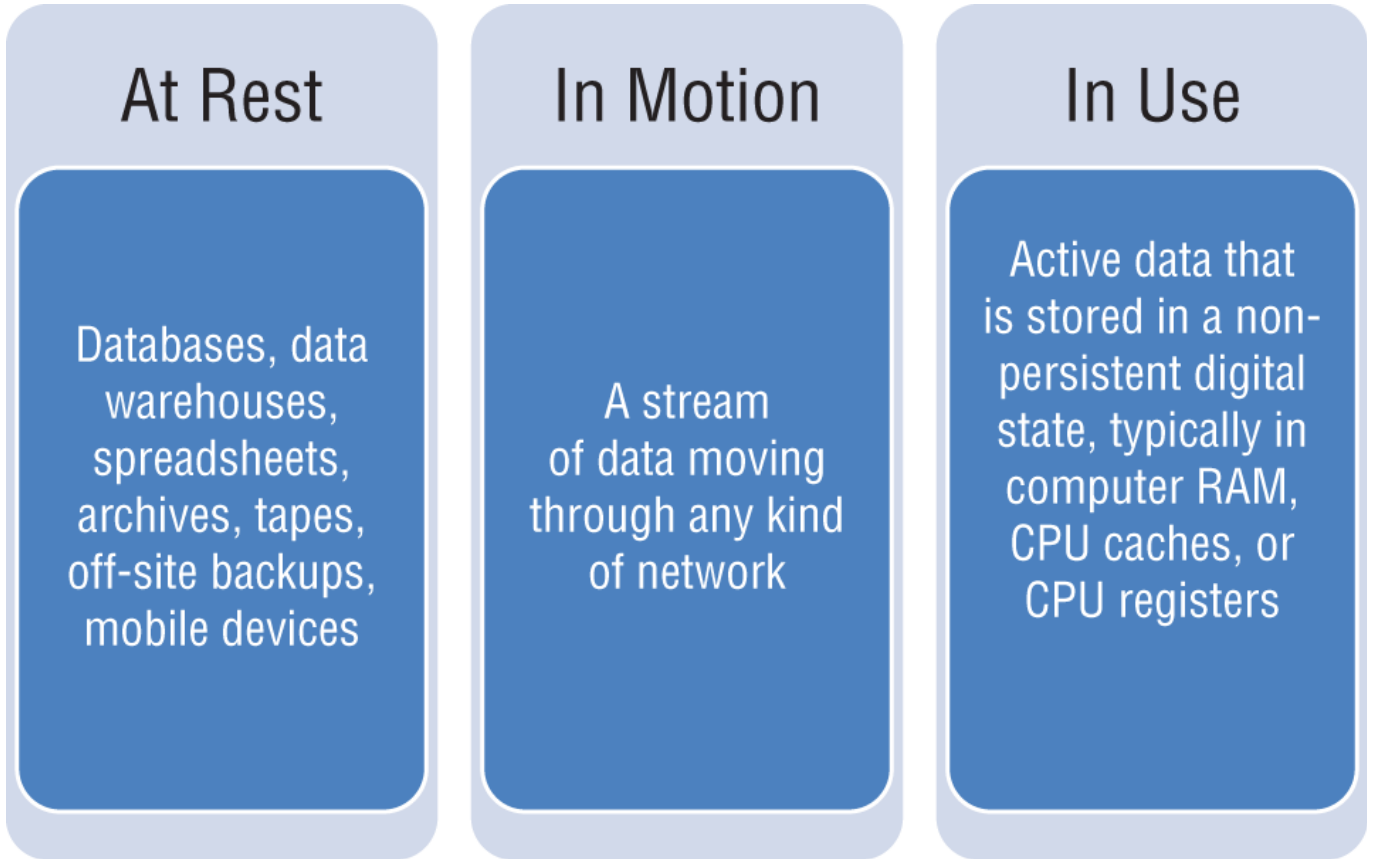
Also discussed Chapter 1

DOMAIN 2: ASSET SECURITY

Data Security Controls

Data States (p. 241-245)

Figure 2.7 Data States and Examples



CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Security Controls

Data Protection – *Data at Rest*

- Access Controls
- Disk / Data Encryption
  - Trusted Platform Module (TPM)
  - Self-encrypting drive (SED)
  - File-level encryption

Encryption is your friend. Covered in Domain 3.

DOMAIN 2: ASSET SECURITY

Data Security Controls

Data Protection – *Data in Transit*

Encryption is your friend. Covered in Domain 3.

- Transport Layer Security (TLS) (including HTTPS)
- VPNs
- Link encryption – Traffic is encrypted and decrypted at each network routing point (e.g., network switch)
- End-to-end encryption – Only sender & receiver can read data

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Security Controls

Data Protection – *Data in Use*

Covered in Domain 3.

- Often forgotten
- Protecting Data being processed
  - Applications (RAM, CPU, Caches, etc.)
  - End users
- Encryption may not be relevant
- Access Control is…

DOMAIN 2: ASSET SECURITY

Data Security Controls

Scoping & Tailoring

- Not synonymous
- Work together to build the configuration baseline.

- ***Scoping*** is the process the organization undertakes to consider which security controls apply and what assets they need to protect.
- ***Tailoring*** is the process of modifying the set of controls to meet the specific characteristics and requirements of the organization.

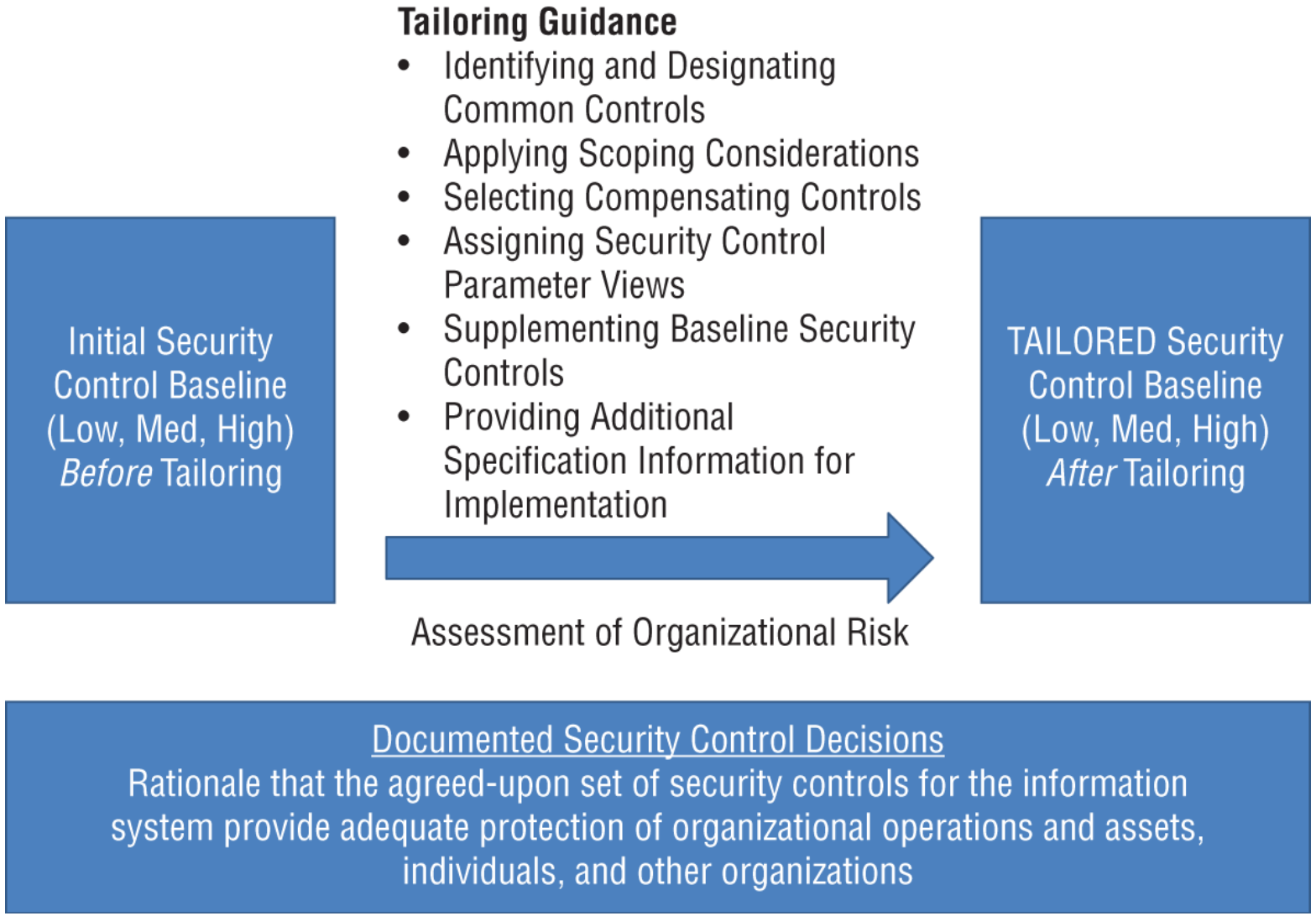
CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Security Controls

Tailoring Process

Figure 2.8, p. 246
from NIST SP800-53



Convenience is not a factor for removing or altering security controls. Make sure any changes to baseline requirements are rationalized against operational requirements and are analyzed for impact to risk

DOMAIN 2: ASSET SECURITY

Data Security Controls

Scoping & Tailoring – *Compensation Security Controls*

- The entity uses an alternative method to achieve the same result.
- NIST Definition: The security and privacy controls implemented in lieu of the controls in the baselines that provide equivalent or comparable protection for a system or organization.
- PCI: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other control

DOMAIN 2: ASSET SECURITY

Data Security Controls

Scoping & Tailoring – *Compensation Security Controls*

PCI: Compensating controls must:

- Meet the intent and rigor of the originally stated PCI DSS requirement
- Provide a similar level of defense as the original PCI DSS requirement
- Be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
- Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.”

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

This is the process of modifying the set of controls to meet the specific characteristics and requirements of the organization:

A. Scoping
B. Tailoring
C. De-identification
D. Retention

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: PRACTICE QUESTION

This is the process of modifying the set of controls to meet the specific characteristics and requirements of the organization:

A. Scoping

B. Tailoring

C. De-identification

D. Retention

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Security Controls & Compliance Requirements

Standards Selection – *Security Frameworks* pp. 249-250

- U.S. Department of Defense Instruction (DoDI): DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" (www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf)
- NIST SP 800-37, "Risk Management Framework" (csrc.nist.gov/publications/detail/sp/800-37/rev-2/final)
- NIST Cybersecurity Framework (CSF) (www.nist.gov/cyberframework)
- UK 10 Steps to Cyber Security (www.ncsc.gov.uk/collection/10-steps)

See Slide 25

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Security Controls & Compliance Requirements

Standards Selection – *Security Standards*

pp. 250-252

In addition to frameworks and industry-specific standards (PCI DSS, HIPAA, GDPR)

- NIST SP 800-53 rev 5, "Security and Privacy Controls for Federal Information Systems and Organizations" (csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)
  SP800-53A rev5 (csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final)
  SP800-53B (https://csrc.nist.gov/publications/detail/sp/800-53b/final)
- FIPS Pub 199 "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS Pub 200 "Minimum Security Requirements for Federal Information and Information Systems"

DOMAIN 2: ASSET SECURITY

Data Security Controls & Compliance Requirements

Standards Selection – *Security Standards*

pp. 252-253

ISO 2700X Family

- ISO 27001, "Information technology – Security techniques – Information security management systems – Requirements"" (www.iso.org/isoiec-27001-information-security.html)
- ISO 27002, "Information Technology: Security techniques – Code of practice for information security controls" (https://www.iso.org/standard/75652.html) ←New version

ISO Standards are copyrighted

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

ISO/IEC 27002:2022 – Section 8, Technical Controls

8.1 User endpoint devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.13 Information backup
8.14 Redundancy of information processing facilities
8.15 Logging
8.16 Monitoring activities
8.17 Clock synchronization
8.18 Use of privileged utility programs
8.19 Installation of software on operational systems
8.20 Networks security
8.21 Security of network services
8.22 Segregation of networks
8.23 Web filtering
8.24 Use of cryptography
8.25 Secure development life cycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles
8.28 Secure coding
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information
8.34 Protection of information systems during audit testing

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Digital Rights Management pp. 254-255

- A set of tools and processes focused on controlling the use, modification, and distribution of intellectual property (IP) throughout its lifecycle.
- DRM allows you to restrict access, editing, copying, and printing of your digital assets.
- *Information rights management* (IRM) - more broadly protects data from unauthorized access by controlling who can view, copy, delete, or otherwise modify data.

DOMAIN 2: ASSET SECURITY

aka Data Leakage Protection

Data Protection Methods

Data Loss Prevention (DLP) pp. 255-258

- Set of technologies and practices used to ensure that sensitive data is not lost or accessed by unauthorized parties.
- Analyzes data storage, identifies sensitive data elements, and prevents users from accidentally or intentionally transmitting sensitive data.

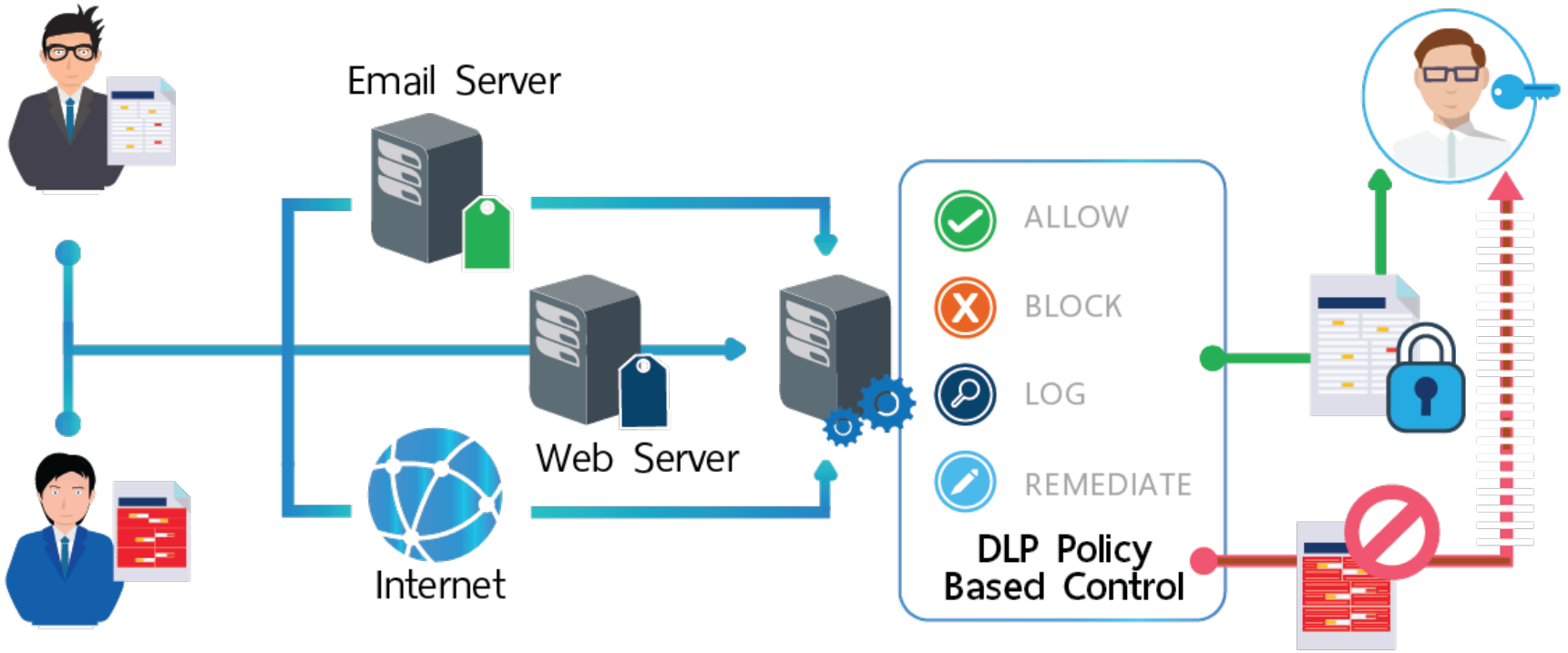
CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

aka Data Leakage Protection

Data Protection Methods

Data Loss Prevention (DLP) pp. 255-258



CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Data Loss Prevention (DLP) pp. 255-256

3 Core Stages:

1. Discovery & Classification
2. Monitoring
3. Enforcement

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Data Loss Prevention (DLP) pp. 257

DLP during 3 States of Data:

1. DLP at Rest – Wherever data is stored
2. DLP in Transit – Network-based DLP
3. DLP in Use – Host-based DLP

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Cloud Access Security Broker (CASB) pp. 258-259

Software application that sits between cloud users and cloud services and applications.

Actively monitor all cloud activity and implement centralized controls to enforce security.

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Cloud Access Security Broker (CASB) pp. 258-259

4 Functions:

1. Visibility – Provide insight into cloud usage
2. Data Security – Monitor & help prevent data exfiltration
3. Threat Protection
4. Compliance

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Cloud Access Security Broker (CASB) pp. 258-259

3 Primary Types of CASB:

1. *Forward Proxy* – Resides on end-points, inspects and forwards cloud traffic for the user. Requires install of certificates.
2. *Reverse Proxy* – Integrates into identity services. Inline monitoring.
3. *API-based* – Monitors data within the cloud itself, rather than on a perimeter-based proxy

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

Not mentioned in Chapter

Data Protection Methods

Integrity Checking

- File Integrity Monitoring (FIM)
- Verifies integrity of systems and files
- Comparing against trusted baselines
- Works with change management procedures.

CISSP® MENTOR PROGRAM – SESSION FOUR

DOMAIN 2: ASSET SECURITY

YAY! 👍
Another Domain done!

Topics:

- Identify and Classify Information and Assets
- Establish Information and Asset Handling Requirements
- Provision Resources Securely
- Manage Data Lifecycle
- Ensure Appropriate Asset Retention
- Determine Data Security Controls and Compliance Requirements

Questions on Domain 2?

pp. 184 - 261

CISSP® MENTOR PROGRAM – SESSION FOUR

SESSION 4 - FIN

We made it!

Next Session (Wed, 27 April 2022) -
Domain 3 (Security Architecture & Engineering) - Ryan

- Research, Implement and Manage Engineering Processes Using Secure Design Principles
- Understand the Fundamental Concepts of Security Models
- Select Controls Based on Systems Security Requirements
- …

CISSP® MENTOR PROGRAM – SESSION FOUR

SESSION 4 - FIN

Homework:

- Review Domain 2 & Domain 3.
- 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 Slack Channel.

See you Wednesday!

CISSP® MENTOR PROGRAM – SESSION FOUR

WHOAMI

Ron Woerner, CISSP, CISM

- Cybersecurity Professor, Bellevue University
- Chief Security Officer, Cyber-AAA

https://linktr.ee/cyberron

https://www.linkedin.com/learning/instructors/ronald-woerner?u=2189410

@ronw123

Hackers Wanted
TEDx Omaha

2022

Class #4 – Domain 2

Ron Woerner

Cyber-AAA Founder & CEO & vCISO
Bellevue University CyberSecurity Studies Professor