2023

Class #3 – Domain 1,2 & 3

Ryan Cloutier

President of SecurityStudio & vCISO
Infosec Missionary on a Mission

CISSP® MENTOR PROGRAM – SESSION THREE

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 #

INTRODUCTION

Agenda –

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

CISSP® MENTOR PROGRAM – SESSION THREE

HELLO, NICE TO MEET YOU

Ryan Cloutier, CISSP, Tonight's Instructor

@cloutiersec
@StudioSecurity

- President of SecurityStudio®
- Virtual Chief Information Security Officer
- Serving the underserved, is my passion
- Speaking human about tech, is my superpower
- Co-host of the Security Shit Show, and Security Simplified podcast
- Infosec Missionary (helper and protector at heart)
- Author
- Advisor to many

CISSP® MENTOR PROGRAM – SESSION THREE

HELLO, NICE TO MEET YOU

Ryan Cloutier, CISSP, Tonight's Instructor

@cloutiersec
@StudioSecurity

- Passionate about your success
- Soft spot for K-12 (those who help)
- Blacksmith, Lego nut, Analog human living a digital life
- Believer, Husband, Father, Continuous learner
- May be the energizer bunny in human disguise

https://www.linkedin.com/in/ryan-cloutier/

https://www.securitystudio.com/

CISSP® MENTOR PROGRAM – SESSION THREE

HELLO, NICE TO MEET YOU

Ryan Cloutier, CISSP, Tonight's Instructor

@cloutiersec
@StudioSecurity

- Passionate about your success
- Soft spot for K-12 (those who help)
- Blacksmith, Lego nut, Analog human living a digital life
- Believer, Husband, Father, Continuous learner
- May be the energizer bunny in human disguise

https://www.linkedin.com/in/ryan-cloutier/

https://www.securitystudio.com/

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 Discord 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 Brad Nigh for teaching last week!

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

Let's get going!

QUESTIONS.

The most common questions 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 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 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 THREE

INTRODUCTION

Before we get too deep into this.

How about a dumb dad joke?

Why do skeletons never take any risks?

Yeah, I know.
That's dumb.

Let's get to it…

INTRODUCTION

Cornerstone Information Security Concepts

Definition of "information security" (don't forget):

Information security is managing risks to the **confidentiality**, **integrity**, and **availability** of information using **administrative**, **physical** and **technical** controls.

"Most organizations overemphasize technical controls to protect confidentiality and do so at the expense of other critical controls and purposes."

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1, 2 & 3

Warning! (lots to cover, lots to memorize, long class)

We are covering 250 slides tonight this one will run long

You must read the book and memorize most of this content

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Information Security Governance

Security Policy and Related Documents

Organizational Policies should reflect compliance requirements.

Organizational Policies should be effective and enforceable

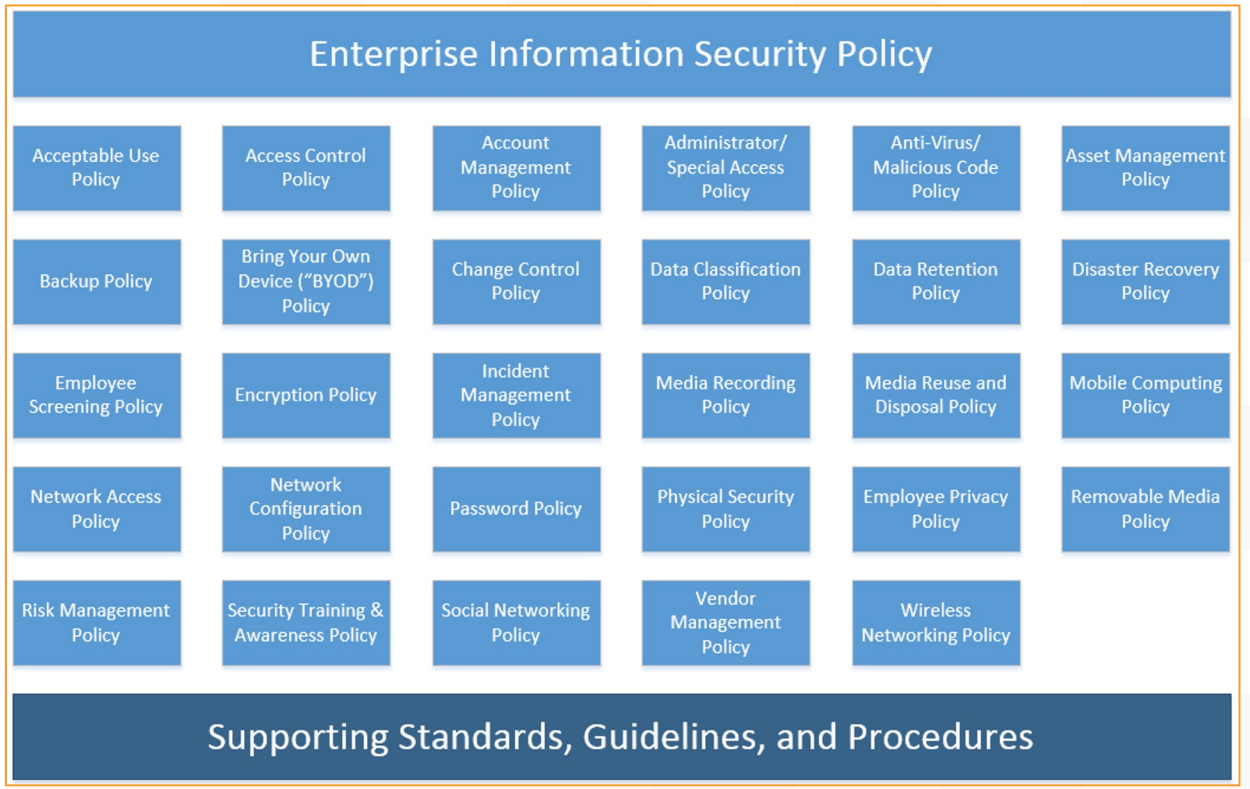
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Security Policy and Related Documents

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



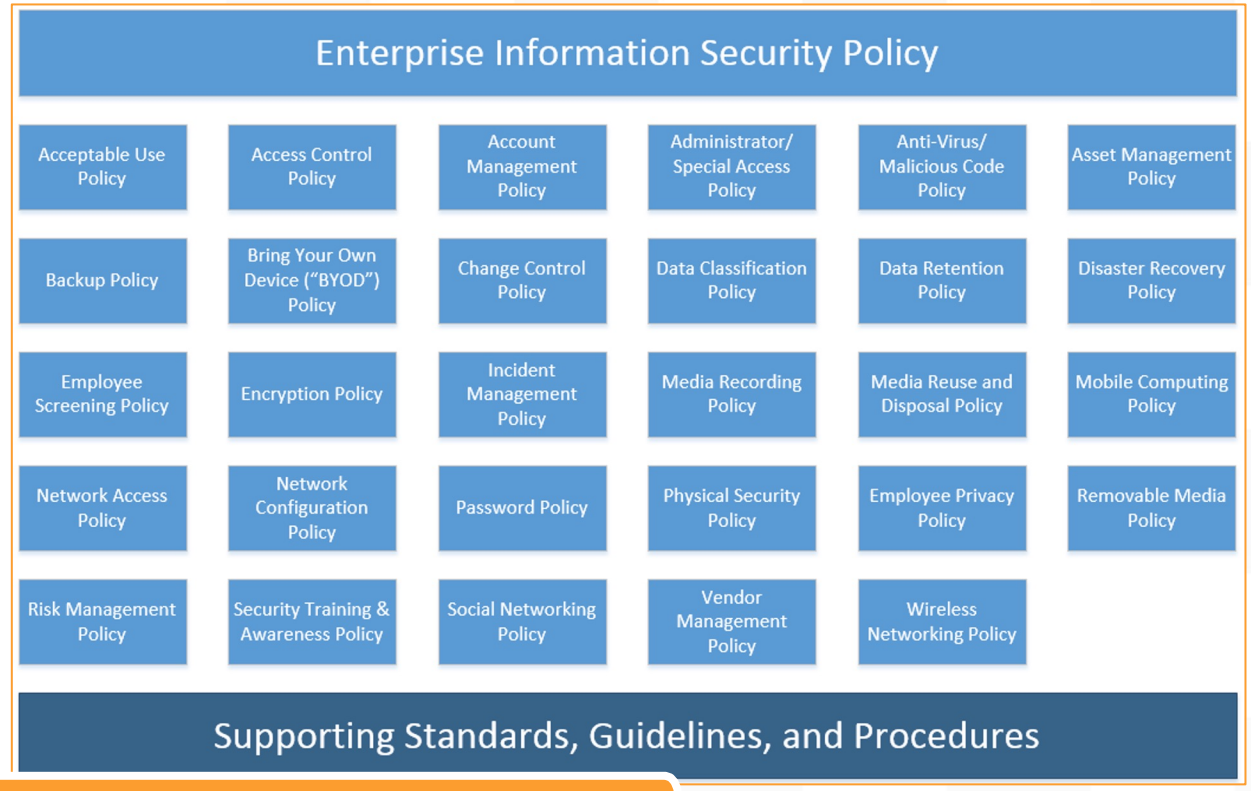
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

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

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

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

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Security Policy and Related Documents

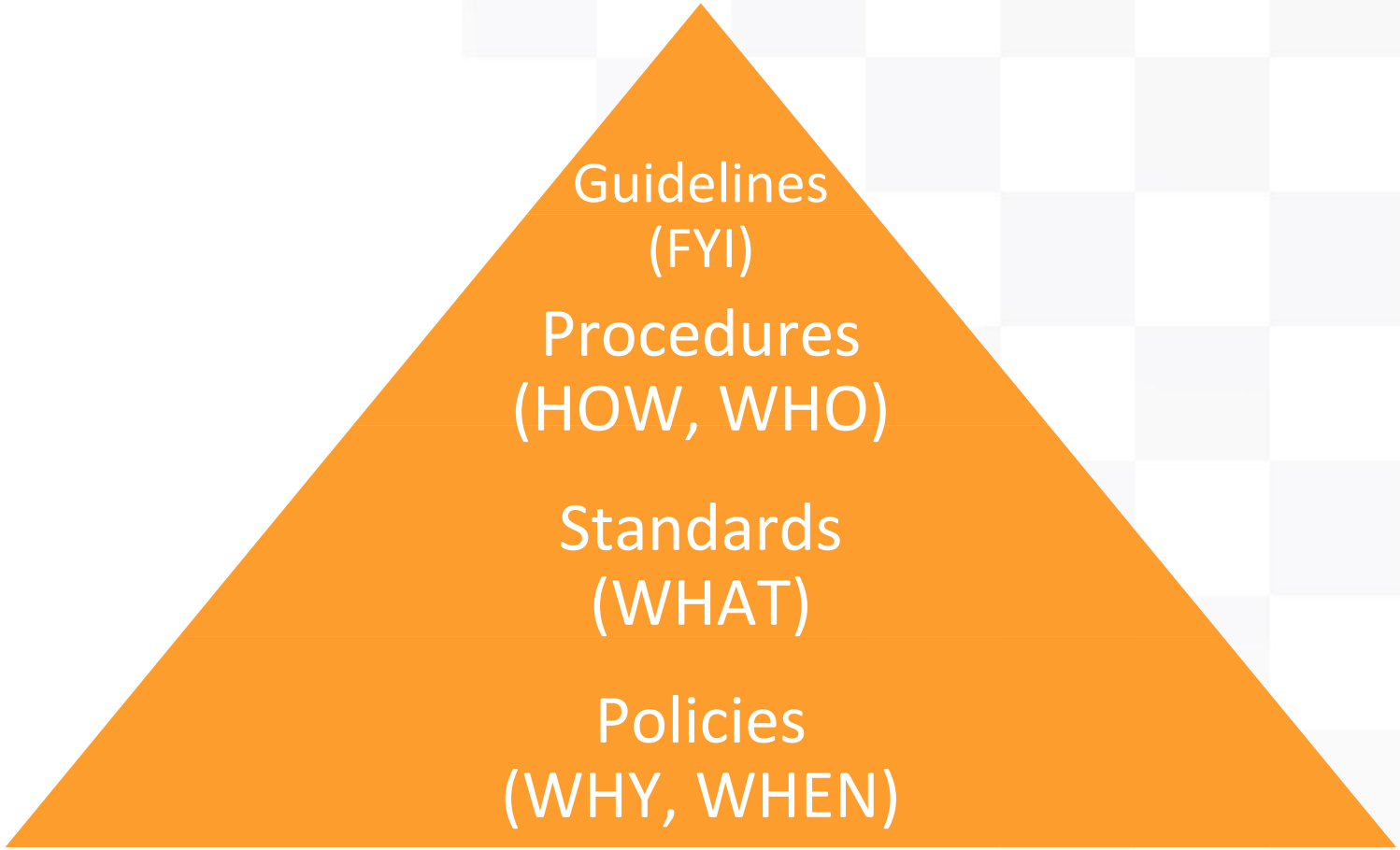
- **Procedures**
  - Mandatory
  - Step-by-step guidance
- **Standards**
  - Mandatory
  - Specific use of a technology
- **Guidelines**
  - Recommendations; discretionary
  - Advice/advisory
- **Baselines** (or benchmarks)
  - Usually discretionary
  - Uniform methods of implementing a standard

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 THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines
Identify, Analyze and Prioritize Business Continuity Requirements

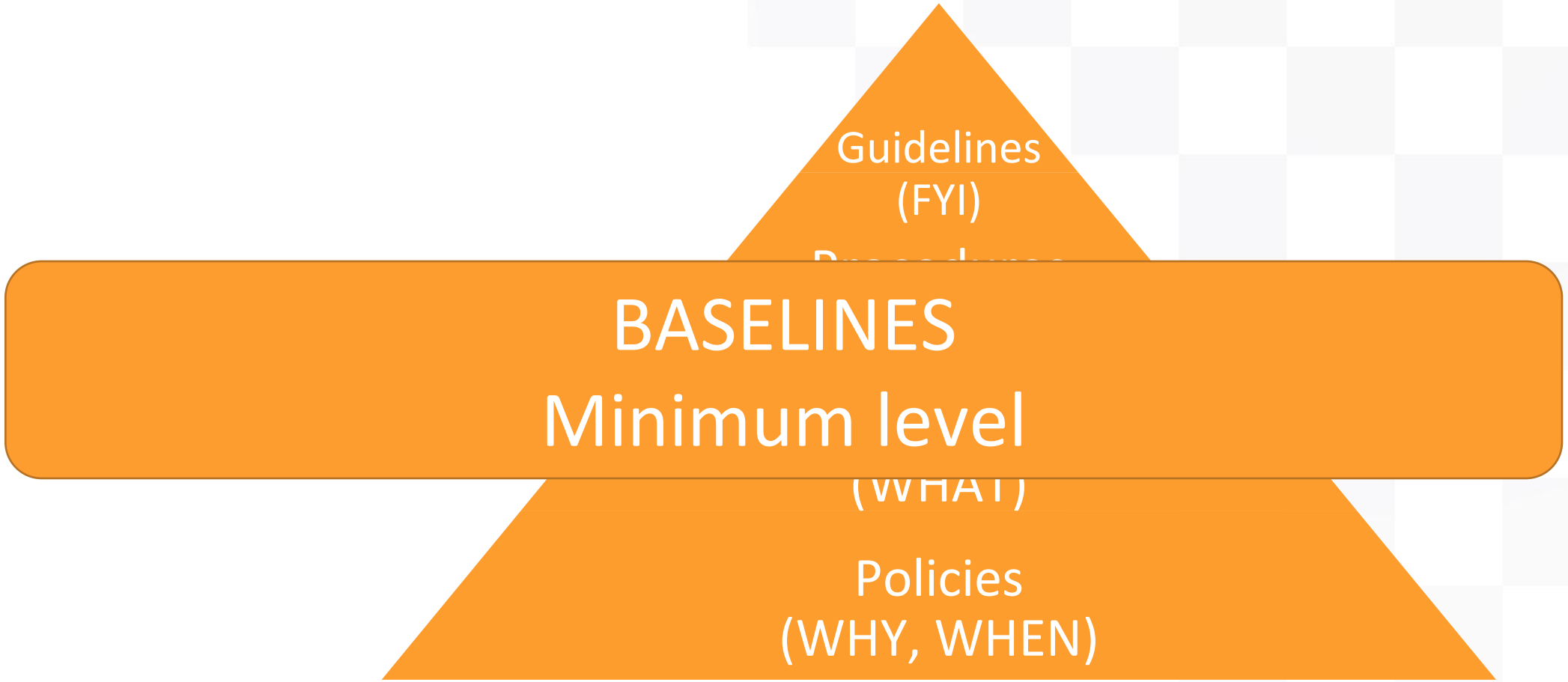


CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines

Identify, Analyze and Prioritize Business Continuity Requirements



DOMAIN 1: SECURITY AND RISK MANAGEMENT

Business Impact Analysis

Identify, Analyze and Prioritize Business Continuity Requirements

BCP Overview and Process

Business Continuity Planning and Disaster Recovery Planning are two very distinct disciplines

Business Continuity Planning (BCP)

Goal of a BCP is for ensuring that the business will continue to operate before, throughout, and after a disaster event is experienced

Focus of a BCP is on the **business as a whole**

Business Continuity Planning provides a **long-term** strategy

Accounting for items such as people, processes and technology in addition to critical systems and data

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Business Impact Analysis

Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Business Continuity Plan (BCP)—a long-term plan to ensure the continuity of business operations

Continuity of Operations Plan (COOP)—a plan to maintain operations during a disaster.

Disaster—any disruptive event that interrupts normal system operations

Disaster Recovery Plan (DRP)—a short-term plan to recover from a disruptive event (more in chapter 7)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Critical Business Function (CBF)—Essential functions critical to the business operations

Business Impact Analysis (BIA)—Analyzing impact of an over time disruption

Maximum Tolerable Downtime (MTD)—Total length of time a critical business function can be unavailable

Maximum Acceptable Outage (MAO)—Total length of time a critical business function can be unavailable

Critical business function is anything the absence of would cause business to stop or be severely interrupted

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Unique terms and definitions

Recovery Time Objective (RTO)—Maximum time to restoration of minimum service expectations, must be less than or equal to MTD

Recovery Point Objective (RPO)—Tolerable amount of data loss in a time period

*not testable

OMG—The feeling you will have executing the BCP plan

FML—what you shout if you didn't print out the BCP plan

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, nts

Unique

Recov ation of

minim to MTD

Recov a loss in a

time p

*not t

OMG-

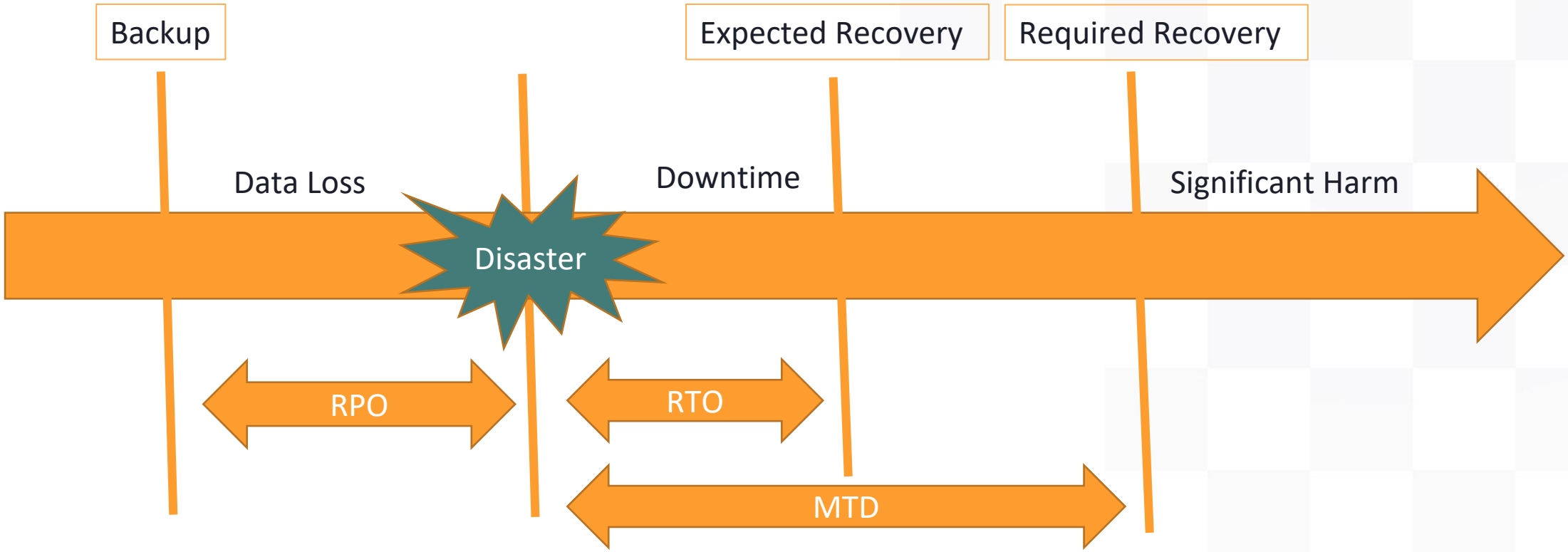
FML—

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements



DOMAIN 1: SECURITY AND RISK MANAGEMENT

Information Security Governance

Identify, Analyze and Prioritize Business Continuity Requirements

Conduct Business Impact Analysis (BIA)

- Formal method for determining how a disruption to the IT system(s) of an organization will impact the organization
- An analysis to identify and prioritize critical IT systems and components
- Enables the BCP/DRP project manager to fully characterize the IT contingency requirements and priorities

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Management Support

"C"-level managers:

- Must agree to any plan set forth
- Must agree to support the action items listed in the plan if an emergency event occurs
- Refers to people within an organization like the chief executive officer (CEO), the chief operating officer (COO), the chief information officer (CIO), and the chief financial officer (CFO)
- Have enough power and authority to speak for the entire organization when dealing with outside media
- High enough within the organization to commit resources

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Develop and Document the Scope and the Plan

- Define exactly what assets are protected by the plan, which emergency events the plan will be able to address, and determining the resources necessary to completely create and implement the plan
- “What is in and out of scope for this plan?”
- After receiving C-level approval and input from the rest of the organization, objectives and deliverables can be determined

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Scoping the Project

- Objectives are usually created as “if/then” statements
  - For example, “If there is a hurricane, then the organization will enact plan H—the Physical Relocation and Employee Safety Plan.” Plan H is unique to the organization but it does encompass all the BCP/DRP subplans required
  - An objective would be to create this plan and have it reviewed by all members of the organization by a specific date.
  - The objective will have a number of deliverables required to create and fully vet this plan: for example, draft documents, exercise planning meetings, table top preliminary exercises, etc.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Scoping the Project

Executive management must at least ensure that support is given for three BCP/DRP items:

- 1. Executive management support is needed for **initiating** the plan.
- 2. Executive management support is needed for **final approval** of the plan.
- 3. Executive management must demonstrate due care and due diligence and be held liable under applicable laws/regulations.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Example Scope

- Critical business functions
- Threats, vulnerabilities, and risks
- Data backup and recovery plan
- BCP personnel
- Communications plan
- **BCP testing requirements**

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

People

- **#1 Most important no exceptions (Life and safety above all else)**
- **Start with human safety then move on**
- **People = Any living human being that may be affected by the event**
- Notifications and communications, using multiple methods
- Resources to keep people working
  - Alternate work locations, food, equipment, internet, etc.
- Regular updates to leadership
- Notifications of external affected parties

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Processes

- What resources need to be available
- Critical supplies (computers, power, internet)
- How do we maintain critical operations
- Logistics
- Continuously available resources
- Recovery site (more in chapter 7)
  - Hot, Warm, Cold
- Testing and updating

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Other Roles

Continuity Planning Project Team (CPPT)

- Comprises those personnel that will have responsibilities if/when an emergency occurs
- Comprised of stakeholders within an organization
- Focuses on identifying who needs to play a role if a specific emergency event were to occur
- Includes people from the human resources section, public relations (PR), IT staff, physical security, line managers, essential personnel for full business effectiveness, and anyone else responsible for essential functions

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Technologies

- **Tech fails plan for it**
- Backups are the #1 way to address this risk
- BCP should account for redundancy (power, water, telco, internet)
- Multiple locations for backups (on-prem and cloud)
- Need to account for external disaster (ISP, Bank, SaaS provider, etc.)
- Testing and updating

CISSP® MENTOR PROGRAM – SESSION THREE

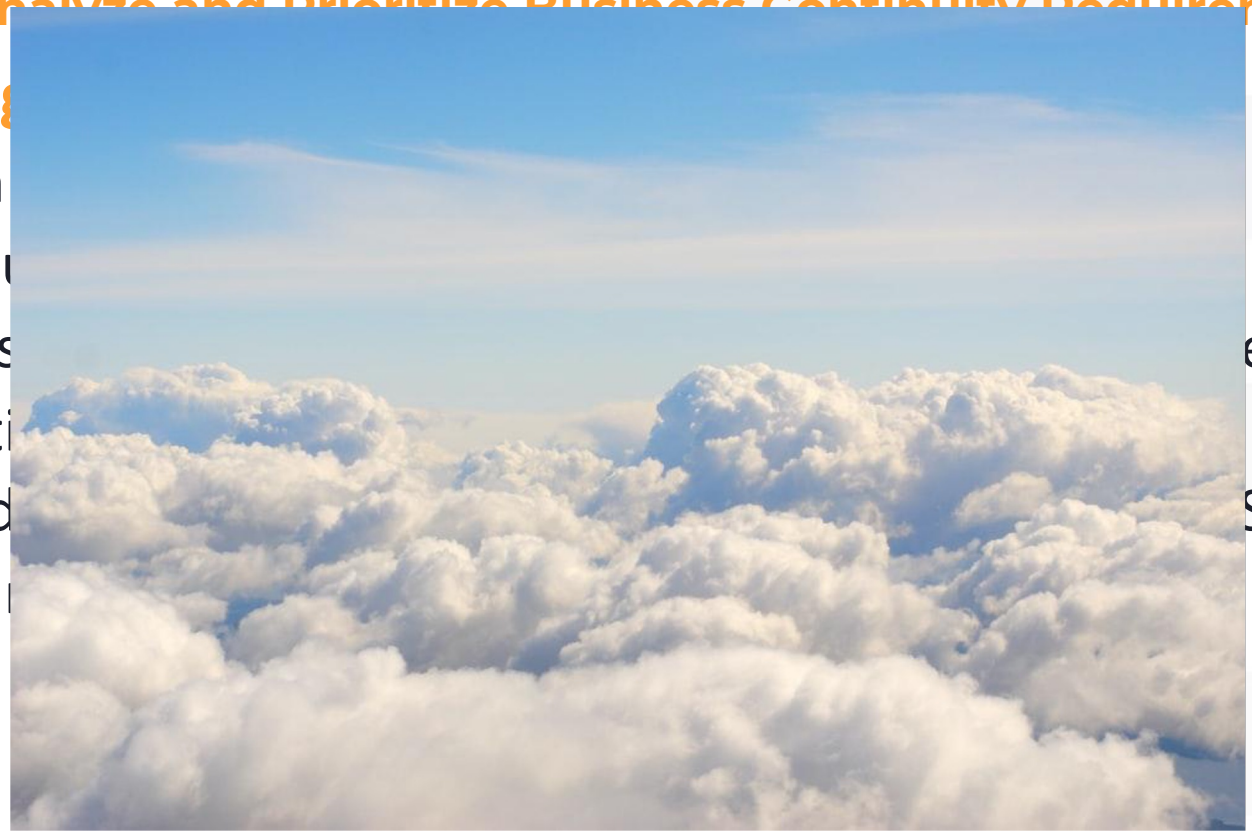
DOMAIN 1: SECURITY AND RISK MANAGEMENT

Develop and Scope the Plan

Identify, Analyze and Prioritize Business Continuity Requirements

Technolog

- **Tech**
- Backu
- BCP s elco, internet)
- Multi
- Need S provider, etc.)
- Testi



DOMAIN 1: SECURITY AND RISK MANAGEMENT

Candidate Screening and Hiring

Contribute to and enforce personnel security policies and procedures

Humans are the biggest part of information security

- Clearly defined roles and job descriptions simplify security
- **Need process and procedure for verifying background**
  - Education, Work history, Citizenship, Criminal record, Credit and financial history, social media activity, and references
- More sensitive positions require further background investigation
- Have clear policies on the use of social media and business systems (appropriate use)
- Verify before granting access to sensitive data

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Employment Agreements and Policies

Contribute to and enforce personnel security policies and procedures

Employment agreements set the stipulations the employee must abide by

- Nondisclosure
- Non compete
- Code of conduct
- Conflict of interest
- Acceptable use
- Employment polices
- Equipment use
- At home expectations (remote worker)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Onboarding, Transfers and Termination process

Contribute to and enforce personnel security policies and procedures

Each stage of employment comes with a security component

- Onboarding sets the tone for work behavior
- Processes for training on secure habits (security awareness)
- Additional training for employees who are likely targets of attackers (C-Level, Admins)
- Process for reporting security incidents (IMO #1)
- Roles and responsibility for securing their work area
- Data classification process and training
- Awareness of monitoring controls
- Their actions matter and make the difference (good or bad)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Onboarding, Transfers and Termination process

Contribute to and enforce personnel security policies and procedures

Transfers

- Clearly defined process for role transfer
- Employee access review (Is current access needed for new role)
- Transition period clearly defined (when is it time to cut off access to previous role)
- Least privilege (enforce)
- Legacy needs (smaller orgs)
- Temporary access (helping out)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Onboarding, Transfers and Termination process

Contribute to and enforce personnel security policies and procedures

Termination (Voluntary and Involuntary separation)

- Voluntary separation is a planned event (2 weeks, retire, good terms)
  - Use a standard checklist (equipment, access, keys, badges, changing codes)

- Involuntary separation is usually an unplanned event and **threat must be assumed**
- Moves very fast, being well coordinated with HR / manager is key
- It is **emotional for all involved**, respect that and plan for it
- When possible, recover any equipment and retain for **potential forensics**
- Remaining **staff need to be informed of termination** and loss of access (don't reset the password for Evan)
- Process for reporting attempted access by terminated employee
- *Insider threat program established and adhered to (UEBA can alert to a rage quit)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Vendor, Consultant and Contractor Agreements and Controls

Contribute to and enforce personnel security policies and procedures

- Vendor, Consultant and Contractor agreements and controls
  - NDA's and other agreements should be in place to protect sensitive information
  - Policies that support monitoring and auditing of access by 3rd parties
  - Policies that require secure connections with 3rd parties who access sensitive data
- Compliance Policy Requirements
  - Ensure all employees are trained and periodical retrained on policies and regulations they need to comply with in the fulfilment of their job duties.
- Privacy Policy Requirements
  - Privacy policy should include what kind of personal data is collected, how it will or will not be used, how it will be stored, maintained, and secured.
- Review and signature by employee that they understand and will comply with company policies and regulations is common practice

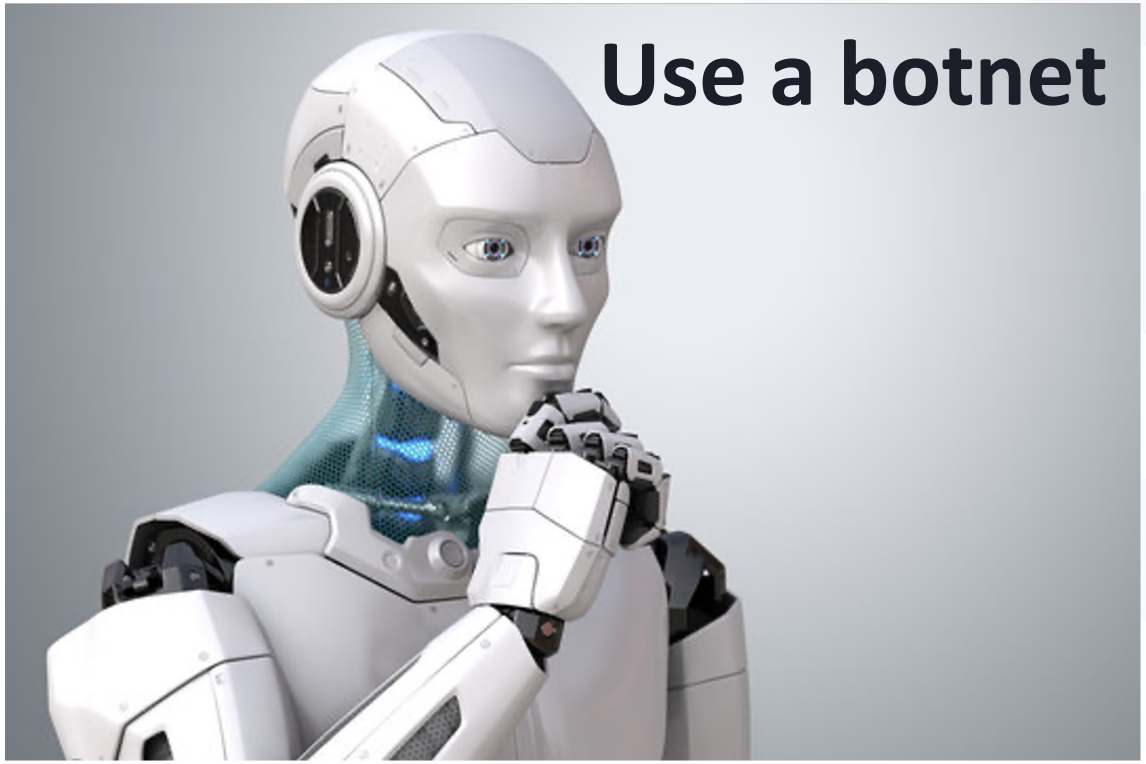
CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKE TIME

Whew that was a lot to take in.

How about a dumb dad joke?

What's the best way to catch a runaway robot?



Yeah, I know.
That's dumb.

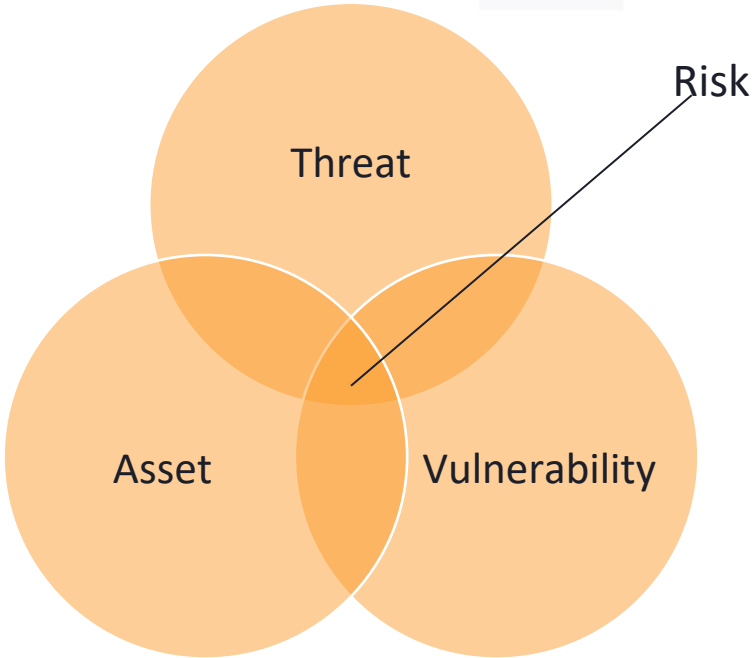
Let's get to it…

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

- Risk management provides structure for making security decisions



CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Information Security IS RISK MANAGEMENT!!!

Unique terms and definitions

Risk—expose (someone or something valued) to danger, harm, or loss.

Inherent risk—risk present before any controls are applied.

Residual risk—level of risk that remains after controls are applied.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Unique terms and definitions

Threats—Negative event leading to a negative outcome.

Examples:

- Fire or natural disaster.
- Disgruntled employee.
- Cybercriminal looking to ransom you.
- Click happy employee

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Unique terms and definitions

Vulnerabilities—Weakness or gap in a system that may be exploited.

Examples:

- Unpatched software applications (#1)
- Weak access control mechanisms (e.g., weak passwords)
- Faulty fire suppression system
- Security unaware employee

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Unique terms and definitions

Vulnerabilities—Weakness or gap in a system that may be exploited.

Examples:

- Unpatched software applications (#1)
- Weak access control mechanisms (e.g., weak passwords)
- Faulty fire suppression system
- Security unaware employee

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Unique terms and definitions

Assets—Anything of value.

- Value can be Quantitative (cost or market value of asset)
- Value can be Qualitative (relative importance to you or the organization)

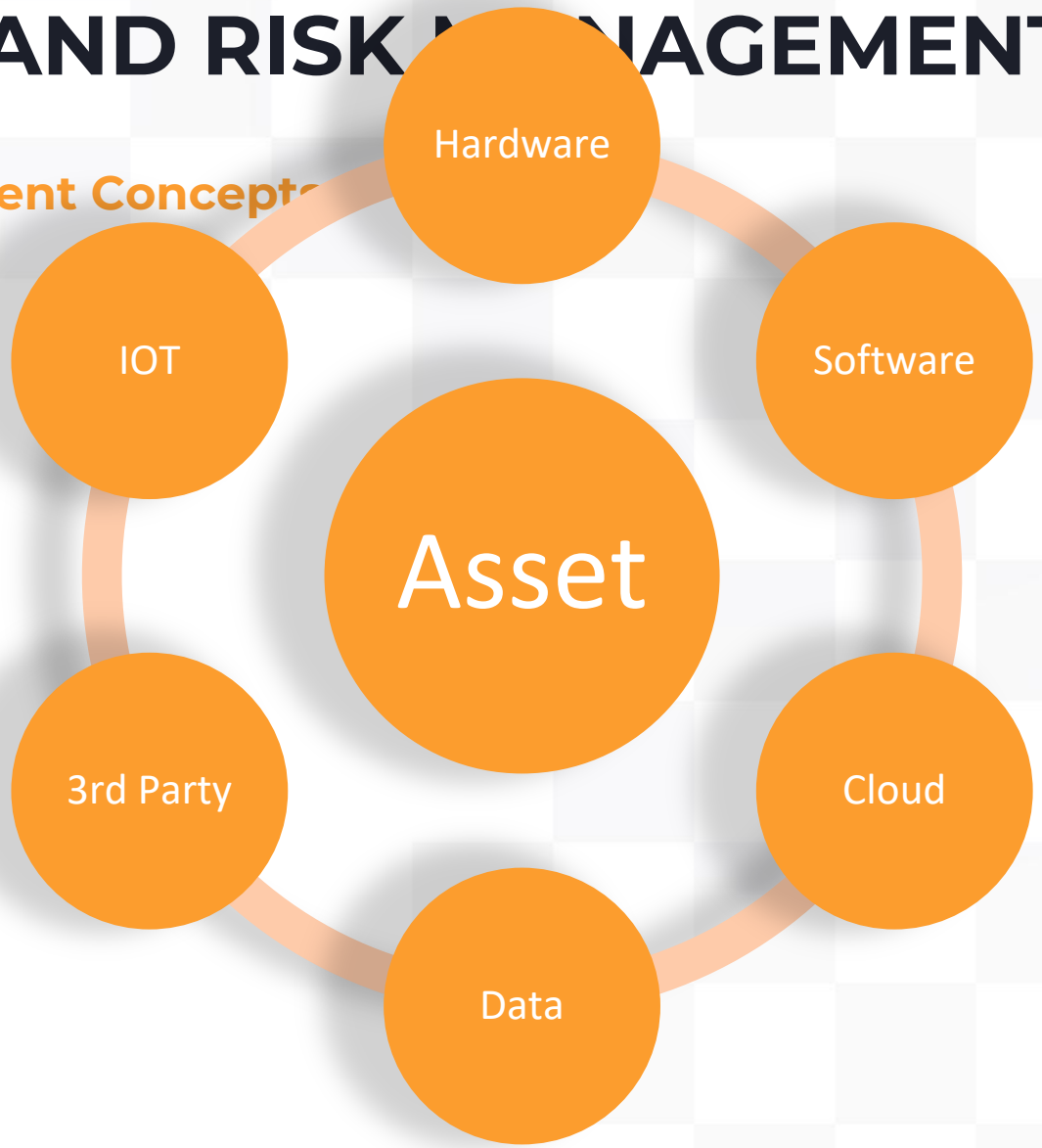
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Unique terms and definitions

Assets—Anything of value.



CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Risk assessments are the gateway to good security

***No such thing as Risk Elimination**

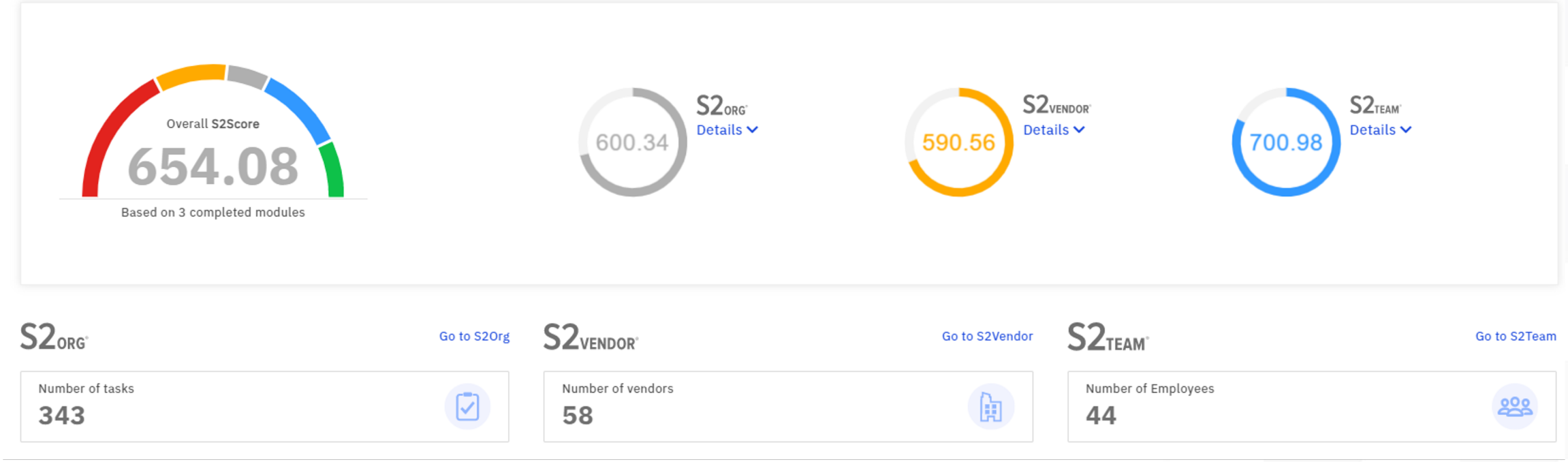
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Risk assessments are the gateway to good security

Overall Results



CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Identification

- Asset discovery (hardware, software, network, data, people)
- Asset valuation (business value of asset)
- Classification (how sensitive, how critical)
- Vulnerabilities and Threats to asset

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Analysis

Should begin with a vulnerability assessment (more in chapter 6) and threat analysis (more on this later in this chapter)

The goal of risk analysis is to evaluate how likely identified threats are to exploit weaknesses (i.e., vulnerabilities)

To make this evaluation we need to look at two key factors

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Analysis

Likelihood—Probability that event will occur.

Impact—How disastrous the event would be if it were to happen .

Risk = Threat x Vulnerability (likelihood and impact)

Risk = Threat × Vulnerability × Impact (another way to put it)

Human life trumps everything!

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities
Understand and Apply Risk Management Concepts

Risk Analysis

- **Qualitative** – based upon professional opinion; High, Medium, Low…
- **Quantitative** – based on real values; dollars. Pure quantitative analysis is nearly impossible (lack of data).
- **Risk Analysis Matrix** – Qualitative risk analysis table; likelihood on one side, impact on the other.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Identify Threats and Vulnerabilities

Understand and Apply Risk Management Concepts

Risk Analysis

5x5 RISK MATRIX

PROBABILITY					
Highly Probable	5 Moderate	10 Major	15 Major	20 Severe	25 Severe
Probable	4 Moderate	8 Moderate	12 Major	16 Major	20 Severe
Possible	3 Minor	6 Moderate	9 Moderate	12 Major	15 Major
Unlikely	2 Minor	4 Moderate	6 Moderate	8 Moderate	10 Major
Rare	1 Minor	2 Minor	3 Minor	4 Moderate	5 Moderate
	Very Low	Low	Medium	High	Very High

IMPACT

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Qualitative & Quantitative Risk Analysis

- **Quantitative** – based on real values; dollars. Pure **Qualitative** analysis is nearly impossible (lack of data).
- **Asset Value (AV)** – Fair market value for an asset
- **Exposure Factor (EF)** - % of asset lost during an incident (threat occurrence)
- **Single Loss Expectancy (SLE)** – **AV** x **EF**
- **Annual Rate of Occurrence (ARO)** – How many times a bad thing is expected/year.
- **Annualized Loss Expectancy (ALE)** – **SLE** x **ARO**

If ALE exceeds Total Cost of Ownership (TCO), there is a positive Return on Investment (ROI), or Return on Security Investment (ROSI).

CISSP® MENTOR PROGRAM – SESSION TWO

INTRODUCTION

Terms and Definitions to Memorize

- **Risk** – The likelihood of something bad happening and the impact if it did; threats (source) and vulnerabilities (weakness)
- **Annualized Loss Expectancy (or ALE)** - the cost of loss due to a risk over a year
- **Safeguard (or "control")** - a measure taken to reduce risk
- **Total Cost of Ownership (or TCO)** – total cost of a safeguard/control
- **Return on Investment (or ROI)** - money saved by deploying a safeguard

Another term is Return on Security Investment or "ROSI".

CISSP® MENTOR PROGRAM – SESSION TWO

INTRODUCTION

Terms and Definitions to Memorize

- **Risk** – The likelihood of something bad happening and the impact if it did; threats (sour[illegible]ness)
- **Annualized Loss** [illegible]st of loss due to a risk over a year
- **Safeguard (or "c** [illegible] reduce risk
- **Total Cost of Ow** [illegible]t of a safeguard/control
- **Return on Invest** [illegible] by deploying a safeguard

Another term is [illegible]ment or "ROSI".

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk Response / Treatment

Understand and Apply Risk Management Concepts

Unique terms and definitions

Risk Tolerance—How much risk the organization is willing to take on.

Risk Profile—How much risk the organization is willing to take on.

Risk Treatment—Best way to address the risk.

Risk Response—Best way to address the risk.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk Response / Treatment

There are only four; risk acceptance criteria should be documented. Risk decisions should **ALWAYS** be made by management, **NOT** information security.

- **Accept** – the risk is acceptable without additional control or change.
- **Mitigate** – the risk is unacceptable (to high) and requires remediation. *(Most common)*
- **Transfer** – the risk can be transferred to someone else; 3rd-party provider, insurance.
- **Avoid** – the risk will be avoided by discontinuing the action(s) that led to the risk.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Countermeasure Selection and Implementation (Security Controls)

Risk mitigation involves ONE or MORE countermeasures with the goal of reducing the likelihood of an adverse event.

- **Personnel-related** – Hiring, Roles, Awareness training.
  - People are the #1 Security risk and #1 Security control
- **Process-related** – Policy, procedure, and workflow-based
  - Separation of duties, dual control
- **Technology-related** – Most of the attention.
  - Encryption, configuration settings, hardware, software, change detection.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Personnel Security Considerations

- Security Awareness and Training
  - Actually two different things
  - Training teaches specific skills
  - Awareness activities are reminders
- Background Checks
  - Criminal history, driving records, credit checks, employment verification, references, professional claims, etc.
  - More sensitive roles require more thorough checks; one-time and ongoing
- Employee Termination
  - Formalized disciplinary process (progressive)
  - Exit interviews, rights revocation, account reviews, etc.
- Dealing with Vendors, Contractors, 3rd Parties
- Outsourcing and Offshoring

Information security isn't about information or security…

As much as it is about people.

1. If people didn't suffer when things go wrong, nobody would (or should) care.

2. People are the most significant risk

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk Response / Treatment

Understand and Apply Risk Management Concepts

Unique terms and definitions

Security-Effectiveness—How effective are the controls selected in addressing the specific risk, and are the controls inline with the kind of security risk your addressing (prevent, detect, or correct)

Cost-Effectiveness—is calculated by performing a cost benefit analysis comparing cost of countermeasure(s) to the cost the would be realized by a compromise of the risks the countermeasures are intended to mitigate.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk Response / Treatment

Understand and Apply Risk Management Concepts

ALE from ransomware event = $200,000

Countermeasure of backups = $50,000

Value added to organization = $150,000

*Countermeasures generally have ongoing costs to factor

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Operational Impact

Understand and Apply Risk Management Concepts

- Countermeasures must be evaluated for impact to the organization
- Difficult to implement or use countermeasures increases risk
- People will circumvent difficult countermeasures
- Understanding culture and strategy is important to selecting countermeasures that don't have a negative operational impact

*Culture and strategy alignment, are a countermeasures best friend

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Applicable Types of Controls

- Categories
  - Administrative Controls
  - Technical Controls
  - Physical Controls
- Types
  - Preventive
  - Detective
  - Corrective
  - Recovery
  - Deterrent
  - Compensating

See! Also in our definition.

VERY TESTABLE: you may be given a scenario or control description and need to provide the category and type.

In order to be sure of the control type, you need to clearly understand context.

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Applicable Types of Controls

- Types
  - **Preventive** – First line controls (firewall, validation, training)
  - **Detective** – Identify negative security event (alarm, IDS, audit)
  - **Corrective** – Minimize and repair damage
    (patching, config management, new or updated policies)
  - **Recovery** – Return to normal ASAP (backups, DR plans)
  - **Deterrent** – Discourage (generally policy, and physical measures)

  - ***Compensating** – Put in place to satisfy a security requirement deemed to difficult or impractical to implement at the present time.
    Not a full mitigation of risk (**encourage vs enforce**)

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKE TIME

Whew that was a lot to take in.

W
an

Bu

Yeah, I know.
That’s dumb.

Let’s get to it…

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Control Assessments

Understand and Apply Risk Management Concepts

Examine – Inspecting, reviewing, observing, studying or analyzing assessment objects.(specifications, mechanisms or activities)

Interview – Talking to people for clarity and obtaining evidence provided during the examine phase.

Test – Comparing actual with expected behavior of the security control, confirming security controls are implemented as they are documented and operating effectively as intended.

Monitoring and Measurement –periodic measuring of security control effectiveness and health (ongoing, annual or quarterly)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Reporting

Understand and Apply Risk Management Concepts

- Process to report to leadership, regulators, and other stakeholders
  - Important discoveries or metrics
- Specific reporting requirements (DHS, Legal, Regulatory, Industry specific)
- A well managed risk-based security program has reporting on
- Internal audits **(self assessment)**
- External audits **(regulators or any other third-party audits)**
- Significant changes to organization's risk posture
- Significant changes to security or privacy controls
- Suspected or confirmed security incidents (or breaches)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Continuous Improvement

Understand and Apply Risk Management Concepts

Strive to improve efficiency of security management program. Seek to continuously improve the ROI associated with security.

Risk maturity modeling assess strength of security program. and informs plans for continuous improvement.

Using a predefined scale S2SCORE helps with focus on specific behavior to improve vs getting caught up in individual security gaps.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks governance considerations

Understand and Apply Risk Management Concepts

- **Consistent** (same way)
- **Measurable** (progress and goals)
- **Standardized** (meaningful comparisons)
- **Comprehensive** (cover the minimum and be extensible)
- **Modular** (withstand change, only modify what you need)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks

Underst

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks

Understand and Apply Risk Management Concepts

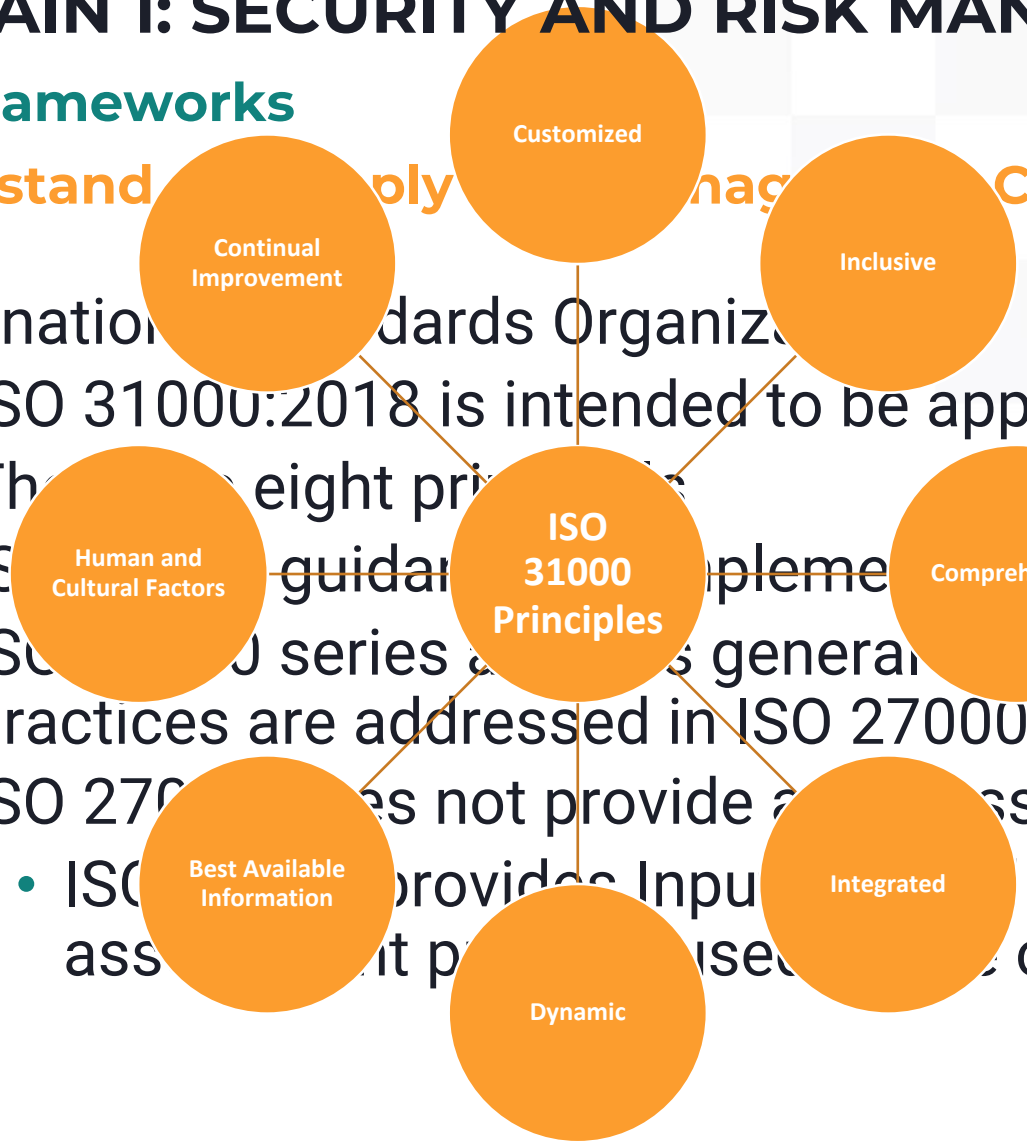
- International Standards Organization
  - ISO 31000:2018 is intended to be applicable to all
  - There are eight principals
  - ISO 31004 guidance on implementing ISO 31000:2018
  - ISO 31000 series address general risk, information security practices are addressed in ISO 27000 series
  - ISO 27005 does not provide a risk assessment practice
    - ISO 27005 provides Inputs to, and outputs from the risk assessment practice used by the organization

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks

Understand ply nag Concepts



- Internatio dards Organiz
  - ISO 31000:2018 is intended to be applicable to all
  - Th eight pri s
  - IS guida pleme 31000:2018
  - ISO 0 series a s genera formation security practices are addressed in ISO 27000 series
  - ISO 270 es not provide a ssessment practice
    - ISO rovide Inpu outputs from the risk ass t p se organization

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks ISO 31000:2018

Understand and Apply Risk Management Concepts

- **Customized** - and proportionate to level of risk
- **Inclusive** - timely involvement of stakeholders
- **Comprehensive** – structured approach is required
- **Integrated** – part of organizational activities
- **Dynamic** – detects, acknowledges and responds to change
- **Best available information** – consider limitations of available information
- **Human and cultural factors** – humans influence all factors
- **Continual Improvement** - improvement through learning

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks

Understand and Apply Risk Management Concepts

- US National Institute of Standards and Technology
  - Risk Management Framework (RMF)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk fr

Unders

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks COBIT and RISKIT

Understand and Apply Risk Management Concepts

- Control Objectives for Information and Related Technology
- Developed by ISACA in the 90's
- Governance of Enterprise IT has 5 processes
- Management of Enterprise IT has 32 processes
- Closely aligned to ISO 20000, ISO 27001, ITIL, Prince2, SOX and TOGAF

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risk frameworks COBIT and RISKIT

Understand and Apply Risk Management Concepts

- RiskIT consists of three domains each with three processes
- Risk governance
- Risk evaluation
- Risk response
- Identifies Organizational responsibilities
- Identifies information flows between processes
- Processes performance management activities
- Additional details in RiskIT Practitioner Guide

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling concepts

Understand and Apply Threat Modeling Concepts and Methodologies

Unique terms and definitions

Threat modeling— Technique to identify potential threats

Threat—Vulnerabilities or absence of necessary security controls

Attack surface— Total area an attacker could execute a compromise

-Information system examples (communications, access control, weakness in system or architecture)

-Physical example (means of entrance egress, construction techniques, location)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling concepts

Understand and Apply Threat Modeling Concepts and Methdologies

- Attacker-centric
- Identify various actors' characteristics, skillset, and motivation
- Profile attackers to specific attacks
- Generally, part of a BCP/DR planning process
- Understanding how the attacker operates

Example: Anti-money laundering process(AML)

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling concepts

Understand and Apply Threat Modeling Concepts and Methdologies

- Asset-centric
- Identify asset value to organization and to the attacker
- The means by which the asset is managed, manipulated, used, and stored
- Evaluate and identify how an attacker might compromise the asset
- Many compliance regimes focus on asset protection (HIPAA,GDPR, PCI-DSS)
- Helpful in protecting other assets such as intellectual property

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling concepts

Understand and Apply Threat Modeling Concepts and Methdologies

- Software-centric (or System-centric)
- This model is most useful
- Systems are represented as asset of interconnected diagrams such as dataflow diagrams (DFD) or component diagrams
- Diagrams are evaluated for potential attacks against each component
- Determine whether a security control is necessary, exists, and achieves the control effect

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling Methodologies STRIDE, PASTA, NIST 800-154 and DREAD

Understand and Apply Threat Modeling Concepts and Methodologies

- **STRIDE**
- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**levation of privilege

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling Methodologies

Understand and Apply Threat Modeling Concepts and Methodologies

- PASTA (**P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis)
- Define objectives
- Define technical scope
- Application decomposition
- Threat analysis
- Vulnerability analysis
- Attack enumeration
- Risk and impact analysis

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling Methodologies

Understand and Apply Threat Modeling Concepts and Methodologies

- NIST 800-154 (Guide to Data-Centric System Threat Modeling)

1. Identify and characterize the system and data of interest
2. Identify and select the attack vectors to be included in the model
3. Characterize the security controls for mitigating the attack vectors
4. Analyze the threat model

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling Methodologies

Understand and Apply Threat Modeling Concepts and Methodologies

- DREAD mnemonic quantitative risk rating

- **D**amage
- **R**eproducibility
- **E**xploitability
- **A**ffected users
- **D**iscoverability

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Threat modeling Methodologies Other Models

Understand and Apply Threat Modeling Concepts and Methodologies

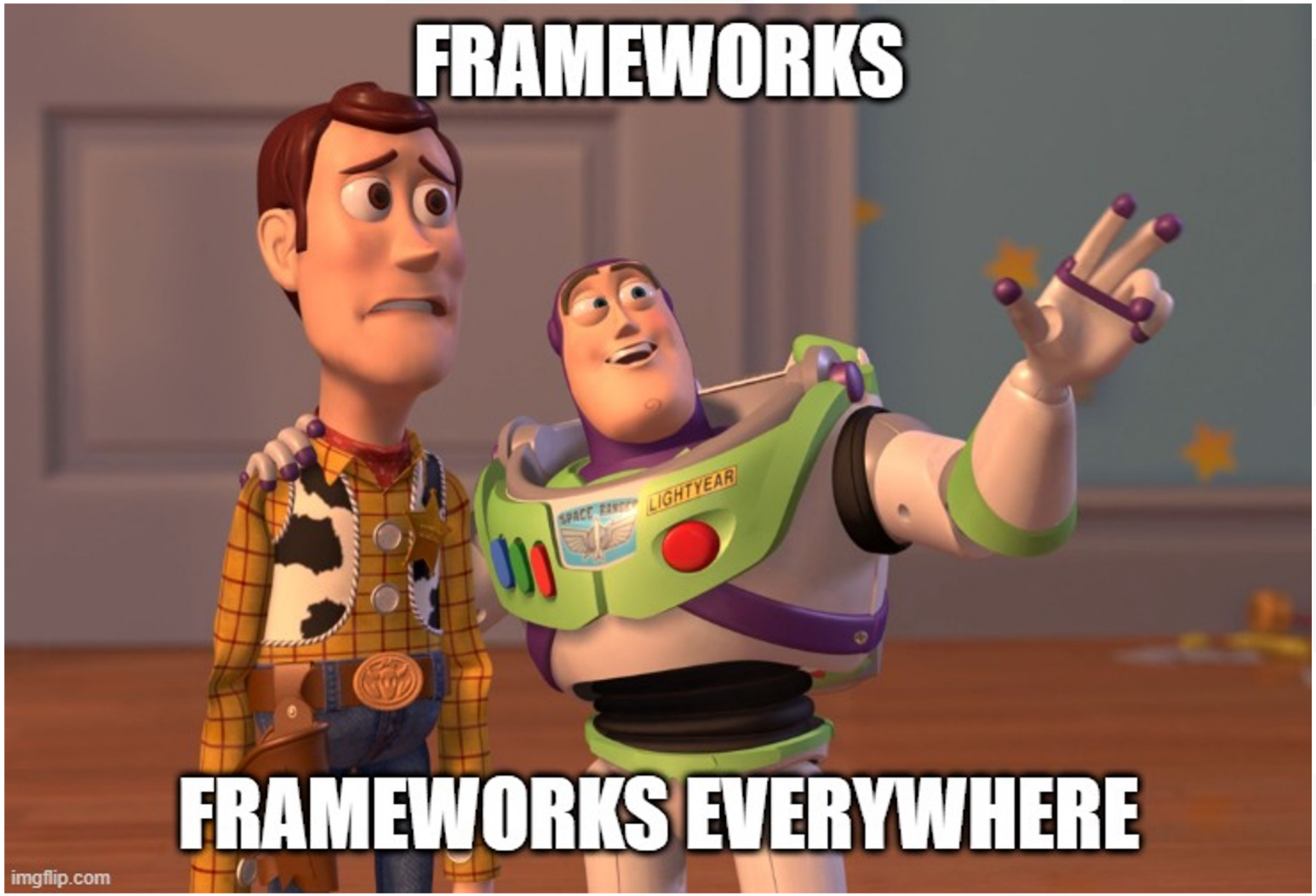
- Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) *developed by Software Engineering Institute (SEI)
- Trike focuses on threat models as risk management tool *open-source
- Construct a platform for Risk Analysis of Security Critical Systems (CORAS) *European project heavy reliance on Unified Modeling Language (UML)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Frameworks

Apply Supply



CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Risks Associated with Hardware, Software and Services

Apply Supply Chain Risk Management Concepts

- Most systems are interconnected and reliant on multiple vendors spread across the globe.
- Must evaluate the entirety of your supply chain and ensure appropriate security controls are in place to manage risk.
- Ensure security controls are aligned to legal, contractual obligations as well as organization polices.

- *cloud is still your responsibility to secure.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Third-Party Assessment and Monitoring

Apply Supply Chain Risk Management Concepts

- Third-parties need to be assessed for risk
- Have a third-party risk management policy that enforces assessing, monitoring and controlling risks.
- Governance and oversight activities should include onsite security surveys, formal security audits of third-party systems and penetration testing.
- New third-parties should be assessed against the organization's security requirements.

*More in chapter 6

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Minimum Security Requirements (MSR)

Apply Supply Chain Risk Management Concepts

- Similar to baselines and standards
- Least acceptable security standards for vendors and others in your supply chain
- Should factor in legal, contractual, or regulatory requirements.
- Ensure the MSR is not below and external security compliance requirement
- Audit and assess third-party compliance with any MSR established

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Service-Level Requirements (SLA)

Apply Supply Chain Risk Management Concepts

- Contractual agreement between service provider and it's customers
- Establishes the minimum performance standards
- Serves as documented and agreed-upon performance requirements
- Generally related to uptime and availability
- Established financial compensation or right to terminate if SLA is not met

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Frameworks NIST IR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems

Apply Supply Chain Risk Management Concepts

- Uniquely identify supply chain elements, process, and actors.
- Limit access and exposure within the supply chain
- Establish and maintain the provenance of elements, processes, tools, and data
- Share information within strict limits
- Perform supply chain risk management awareness and training

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Frameworks NIST IR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems

Apply Supply Chain Risk Management Concepts

- Use defensive design for systems, elements, and processes
- Perform continuous integrator review
- Strengthen delivery mechanisms
- Assure sustainment activities and processes.
- Manage disposal and final disposition activities throughout the system or element lifecycle.

- *National Security Systems Directive 505 “Supply Chain Risk Management”

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Frameworks ISO 28000:2007

Apply Supply Chain Risk Management Concepts

- Not specific to cybersecurity
- Good for organizations using other ISO standards (ISO 9001, ISO 27001)
- Relies heavily on continuous improvment model of Plan, Do, Check, Act (PDCA)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Frameworks U.K. National Cyber Security Center (NCSC)

Apply Supply Chain Risk Management Concepts

- 12 principals divided into three stages
- Understand your risks
- Establish control
- Check your arrangements
- Continuous improvement

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Methods and Techniques to Present Awareness and Training

Establish and Maintain a Security Awareness, Education and Training Program

- Social Engineering
- Security Champions
- Gamification

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Methods and Techniques to Present Awareness and Training

Establish and Maintain a Security Awareness, Education and Training Program

- Social Engineering – Technique of exploiting human weakness
- Phishing is most common method
- Vishing (voice-based phishing)
- Smishing (SMS or text-based phishing)
- Social media (spirit animal survey)
- Impersonation (deep fake, mimicking writing styles)
- User must be trained on what to look for and how to report suspected attempts of social engineering

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Methods and Techniques to Present Awareness and Training

Establish and Maintain a Security Awareness, Education and Training Program

- Security Champions act as a liaison between security and the rest of the company
- Is an advocate of security best practices
- Does not work on security team as part of their primary job
- Should have one per team/ department if team /department is large enough

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Methods and Techniques to Present Awareness and Training

Establish and Maintain a Security Awareness, Education and Training Program

- Gamification is using game techniques in a nongame applications
- Helps bring some fun to awareness training
- Makes security more relatable
- Improves engagement

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Periodic Content Reviews

Establish and Maintain a Security Awareness, Education and Training Program

- Constant change is the norm
- Review and update awareness content regularly to ensure alignment to and coverage of emerging threats
- At a minim annual reviews should be conducted
- Remove any outdated terms and or technology references
- Should reflect current security trends, concepts, and concerns.
- CISSP's should be involved in the development of training content

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SECURITY AND RISK MANAGEMENT

Program Effectiveness Evaluation

Establish and Maintain a Security Awareness, Education and Training Program

- Security awareness training programs should be formally evaluated for effectiveness
- Training metrics (completed, not started)
- Quizzes (testing to understanding)
- Security awareness day or week (capture feedback)
- Inherent evaluation (reporting of suspected security events)

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 1: SEC NT

Program Effectiv

Establish and Maint d Training Program

- Security awaren rmally evaluated for ef
- Training metric
- Quizzes (testing
- Security awaren)
- Inherent evalua y events)

CISSP® MENTOR PROGRAM – SESSION THREE

SESSION 2 - FIN
YOU MADE IT!

Domain 1 is a done WHOOT HECK YA!! YALL!

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

Next Session - Domain 2 (Asset Security) –Ryan

- Identification and classification Information and Assets
- Asset handling requirements
- Provision and inventory
- Management
- Roles
- Data Lifecyle and controls

CISSP® MENTOR PROGRAM – SESSION THREE

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…

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)**

- 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**

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

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.

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

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.

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 THREE

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!

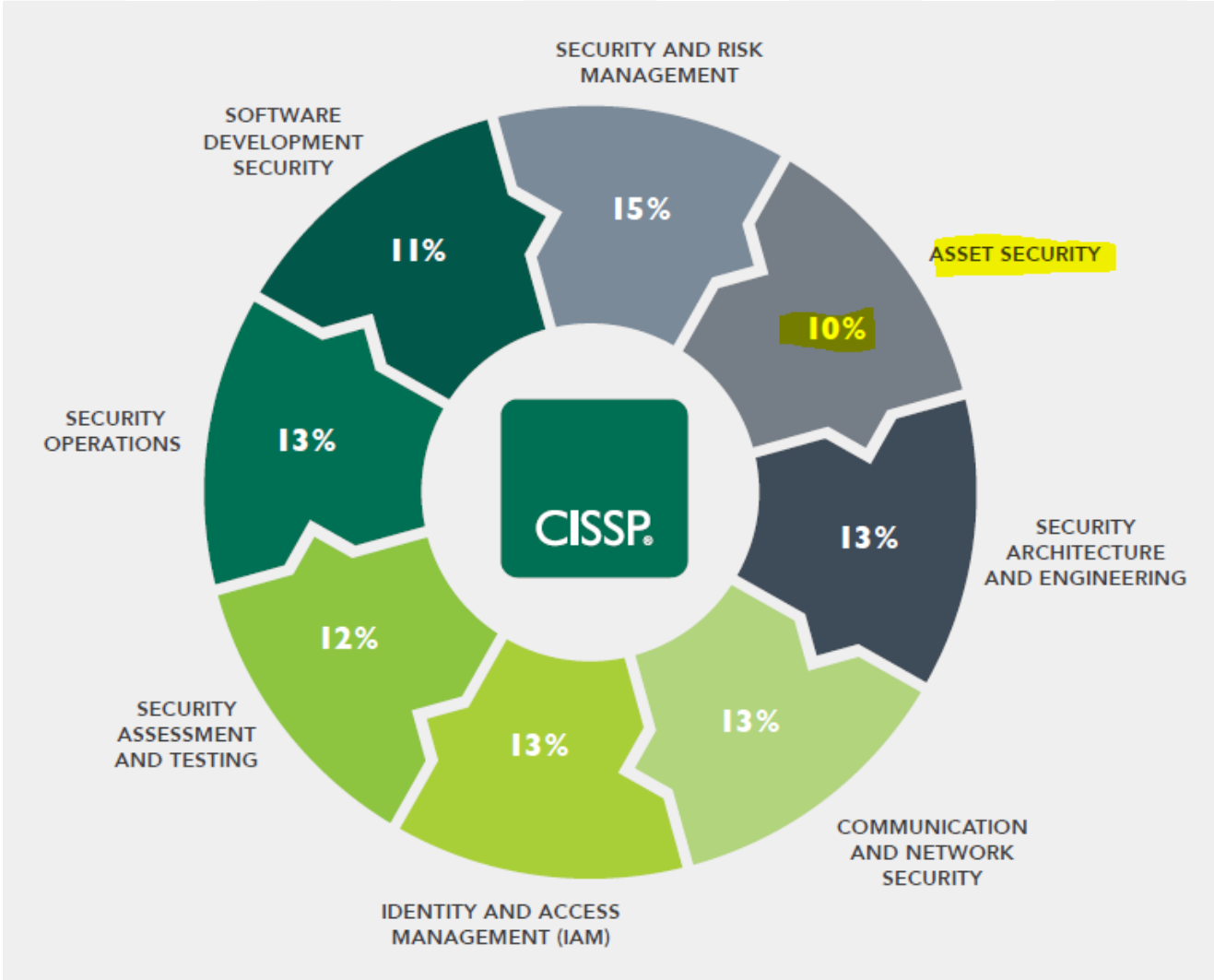
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

CISSP Exam Overview

https://www.isc2.org

Caution!
Concepts overlap between domains.



CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

CISSP Exam Overview

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

You must know what you have 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

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 THREE

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 must know what you have to keep it secure...
And how important it is...

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

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

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

COMPUTER SECURITY RESOURCE CENTER

CSRC

https://csrc.nist.gov/

More about this later

https://www.nist.gov/cyberframework

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

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

https://www.cisecurity.org/

Consensus-developed secure configuration guidelines for hardening.

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

DOMAIN 2: ASSET SECURITY

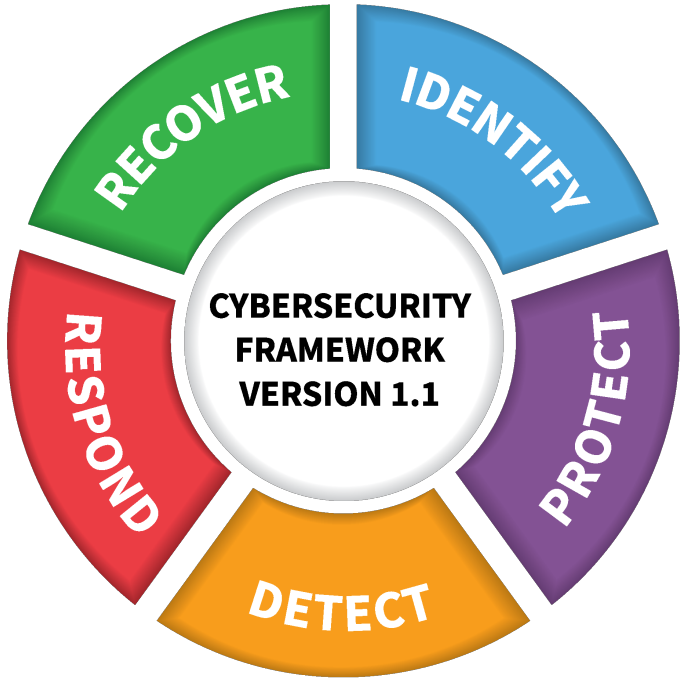
Before I go to far, a couple of **supplemental references**:

What do they have in common?

INVENTORY & ASSET MANAGEMENT

CISSP® MENTOR PROGRAM – SESSION THREE

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 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 THREE

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 THREE

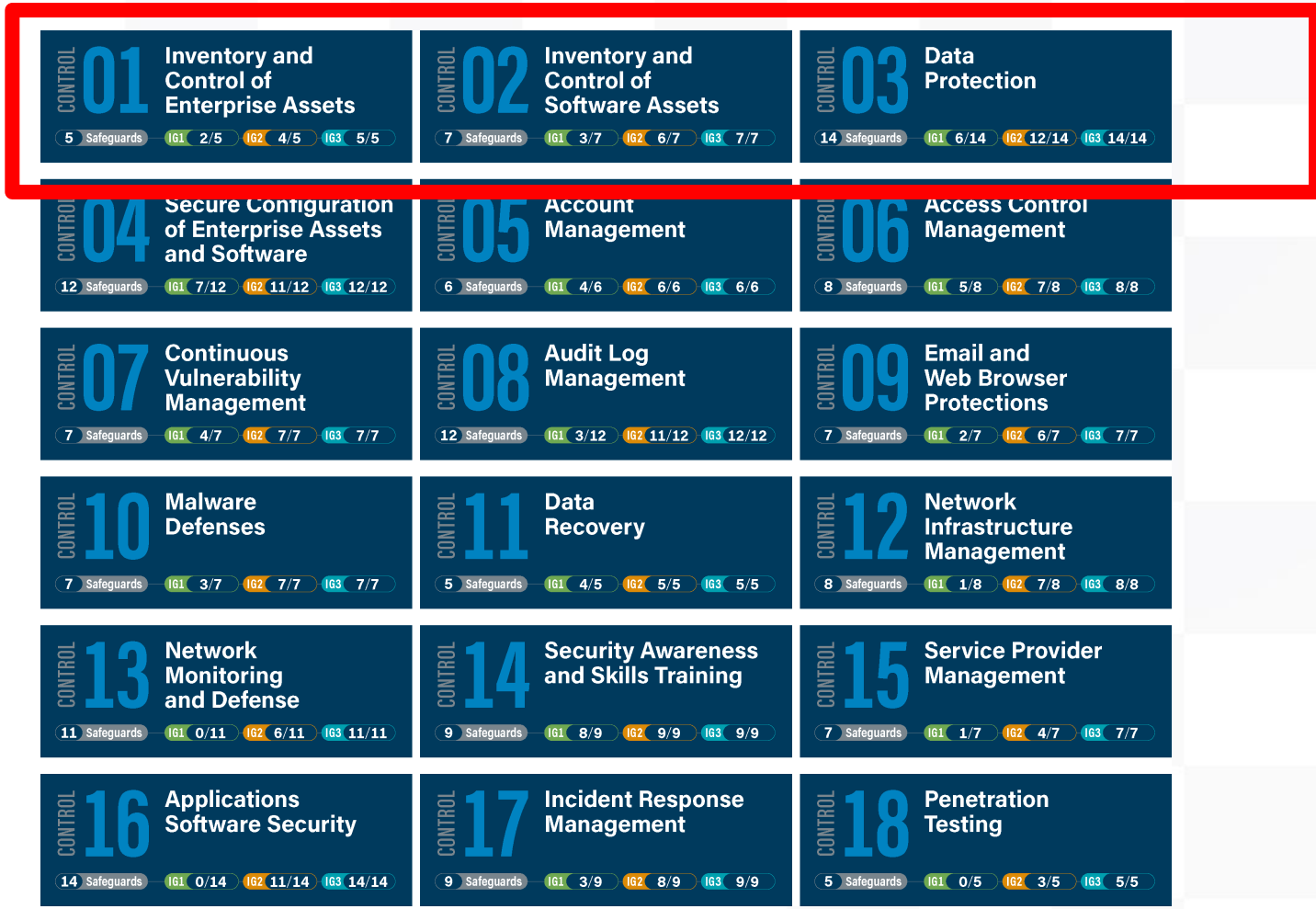
DOMAIN 2: ASSET SECURITY

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”

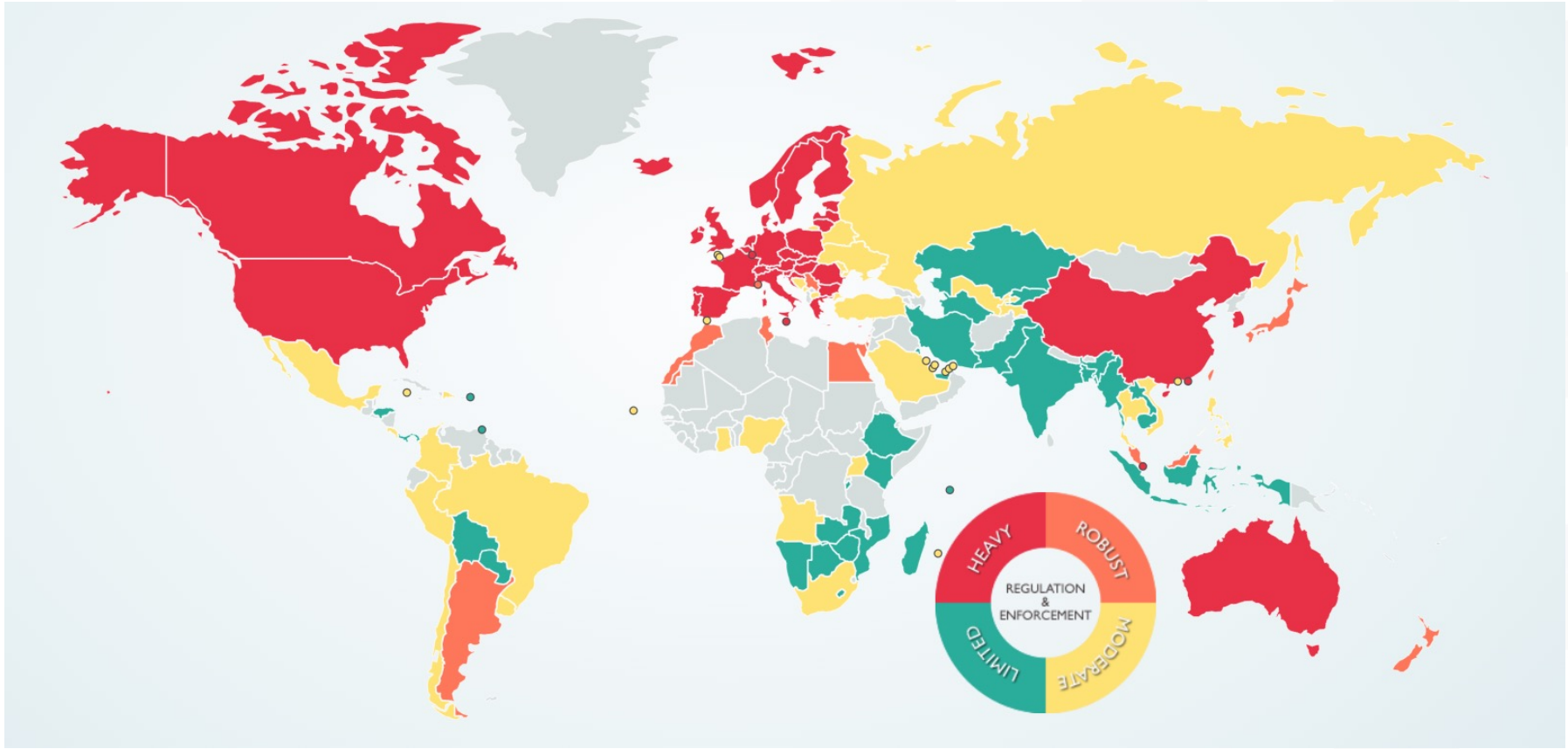
United States: NIST Special Publication (SP) 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”

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

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

Global Privacy Laws

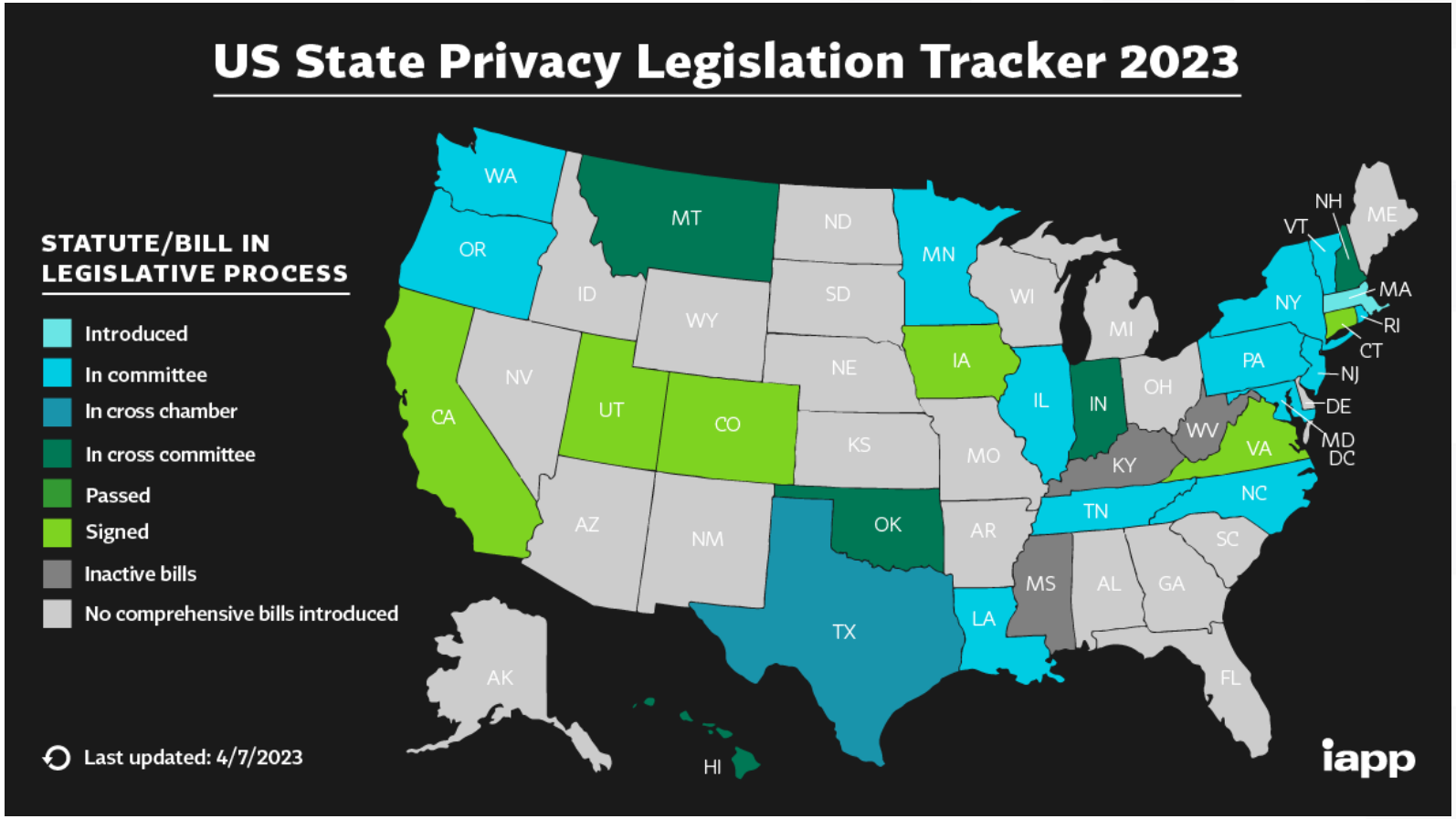


https://www.dlapiperdataprotection.com/

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

US Privacy Laws



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

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)

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)

DOMAIN 2: ASSET SECURITY

Data Lifecycle (p. 214)

Before we talk about Data Classification…

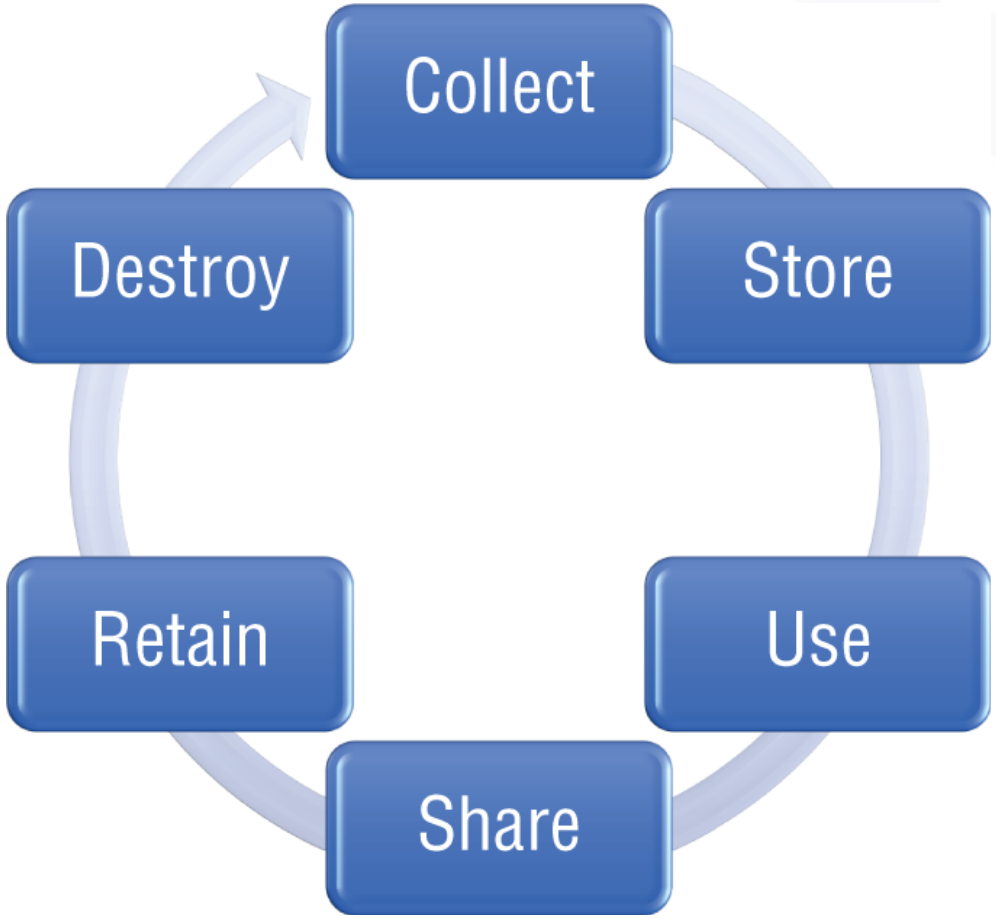


FIGURE 2.5 Secure data lifecycle

CISSP® MENTOR PROGRAM – SESSION THREE

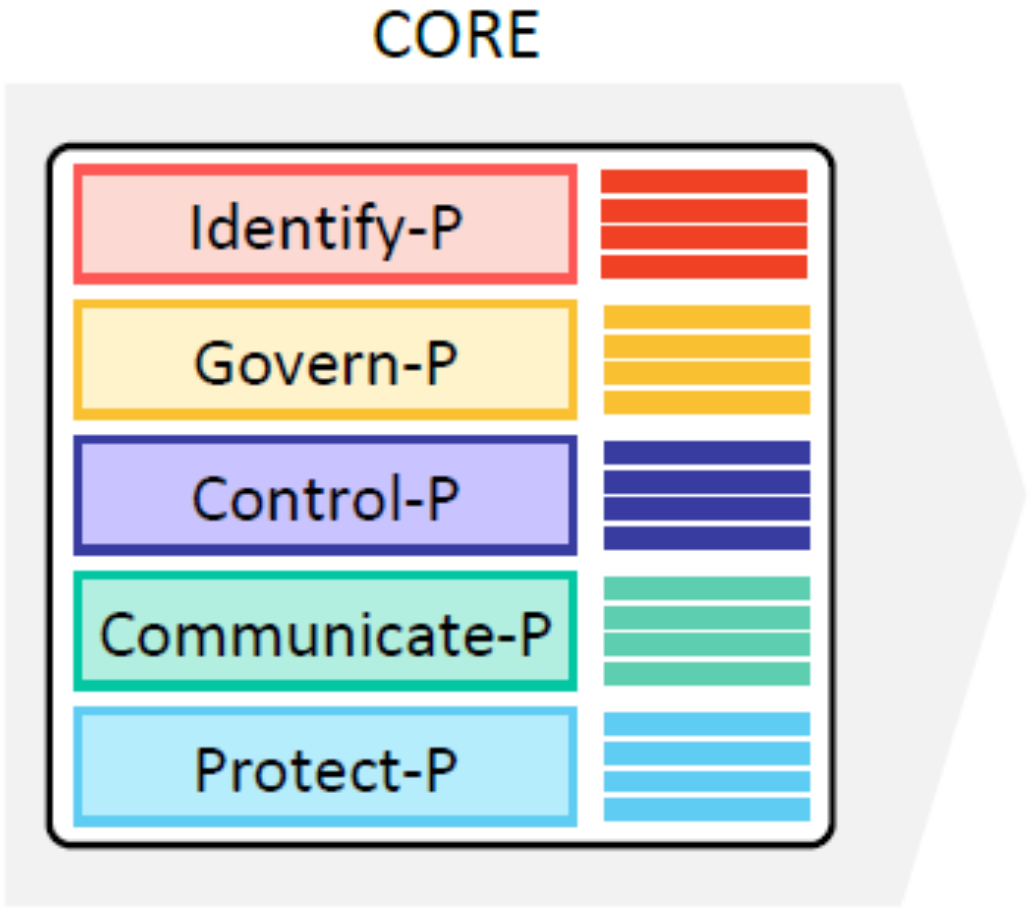
DOMAIN 2: ASSET SECURITY

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.

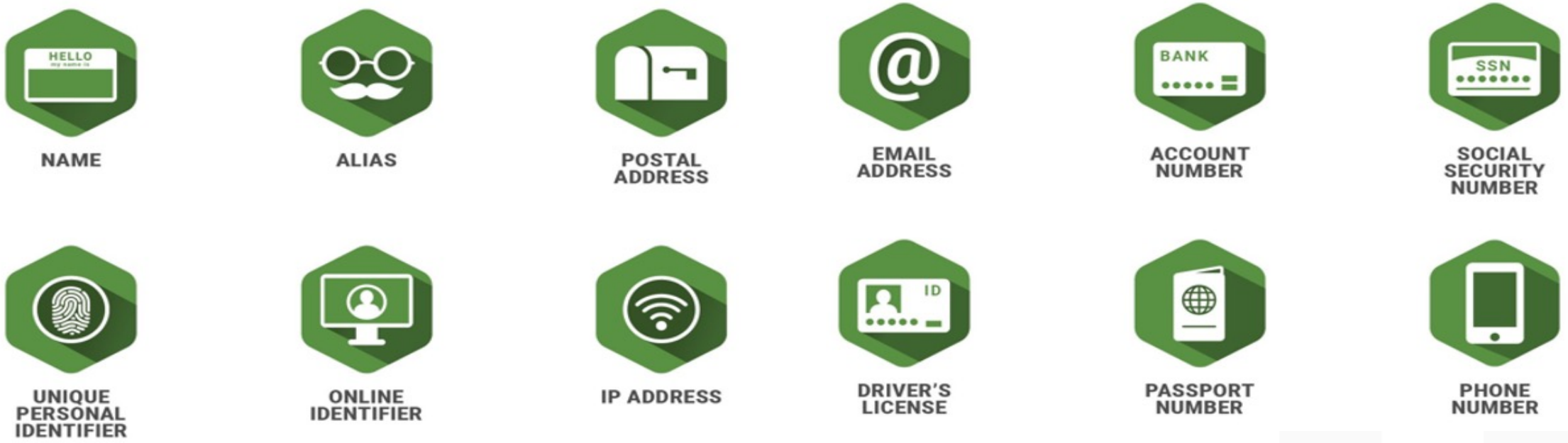
- Three Types:
  - Content-based (e.g., PII, PHI, CHD)
  - Context-based (e.g., Web browsing)
  - User-based

CISSP® MENTOR PROGRAM – SESSION THREE

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 2023 Class 3 Slides & Video

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

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**]

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

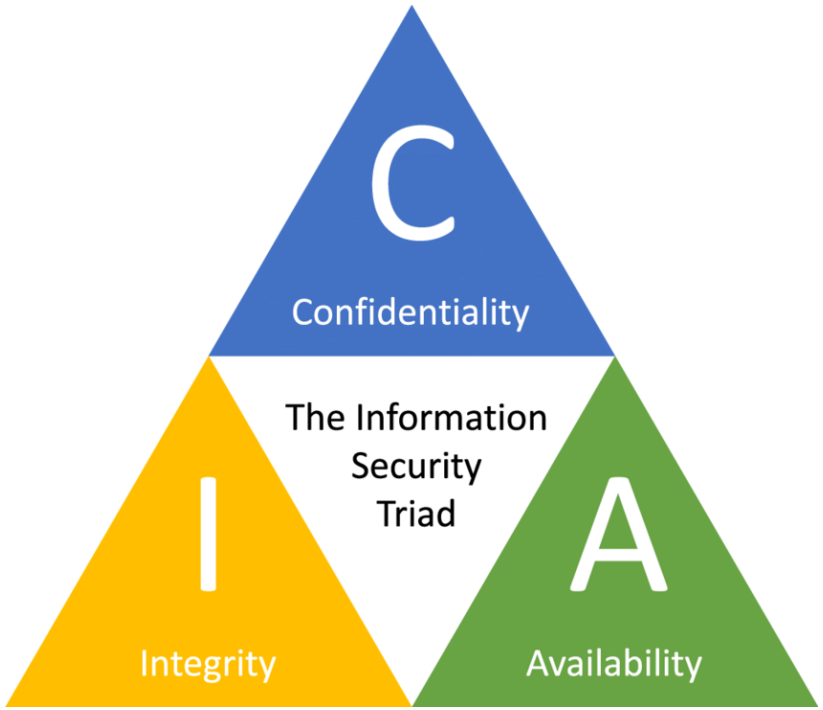
Asset Classification (p. 190)

- 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.

DOMAIN 2: ASSET SECURITY

Identify and Classify Information and Assets

Consider CIA when classifying / categorizing data and assets.



Example: Website

DOMAIN 2: ASSET SECURITY

Classification Benefits (p. 192)

FIGURE 2.1 General benefits of asset classification

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 THREE

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 Discord.

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

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*

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 THREE

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 THREE

DOMAIN 2: ASSET SECURITY

Information and Asset Handling – Storage

Secure Asset Storage

Physical Security

Encryption

Only store data that's needed.

Backups

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.

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

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

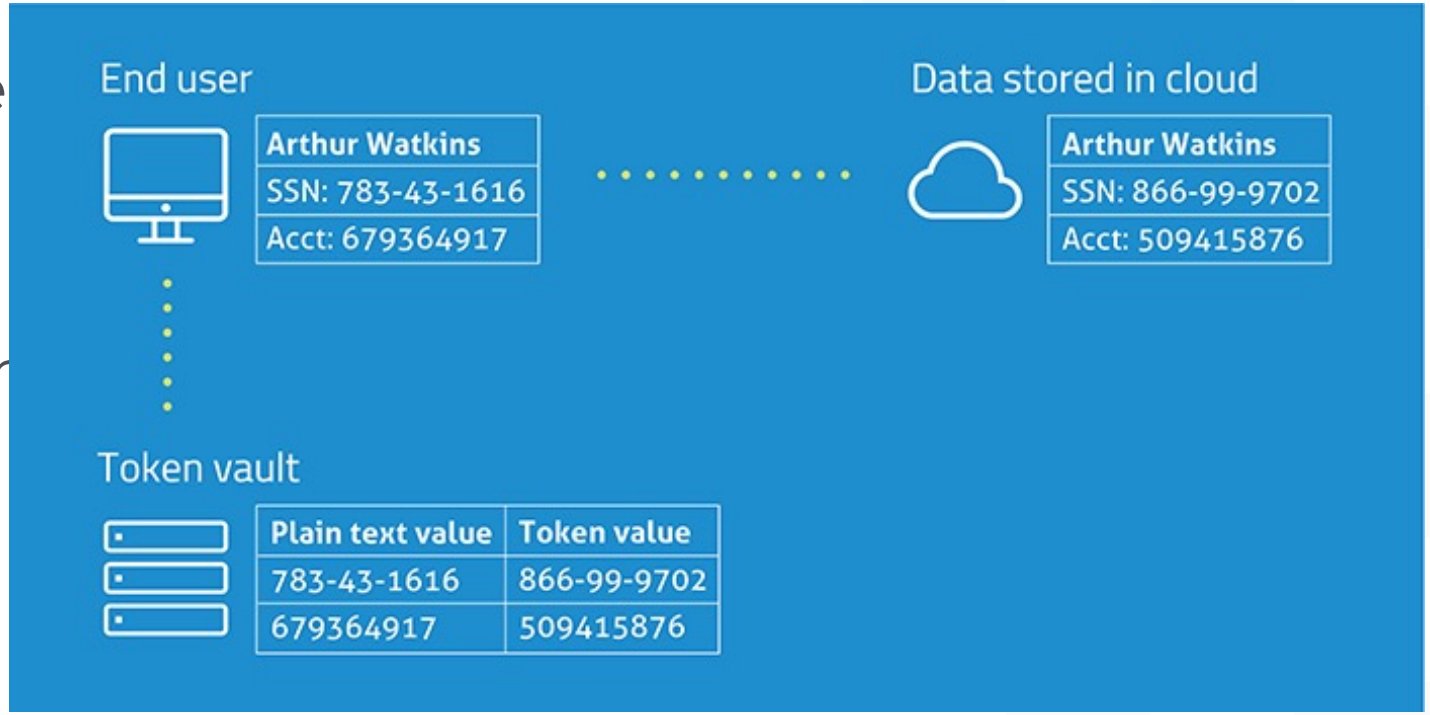
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

Data Declassification Methods (pp. 199-202)

Data Tokenization

- Substituting personal data with a random token
- Link between toke
- Random numbers
- Can't be reverse-er



CISSP® MENTOR PROGRAM – SESSION THREE

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.

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 THREE

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 32cccc

- 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)

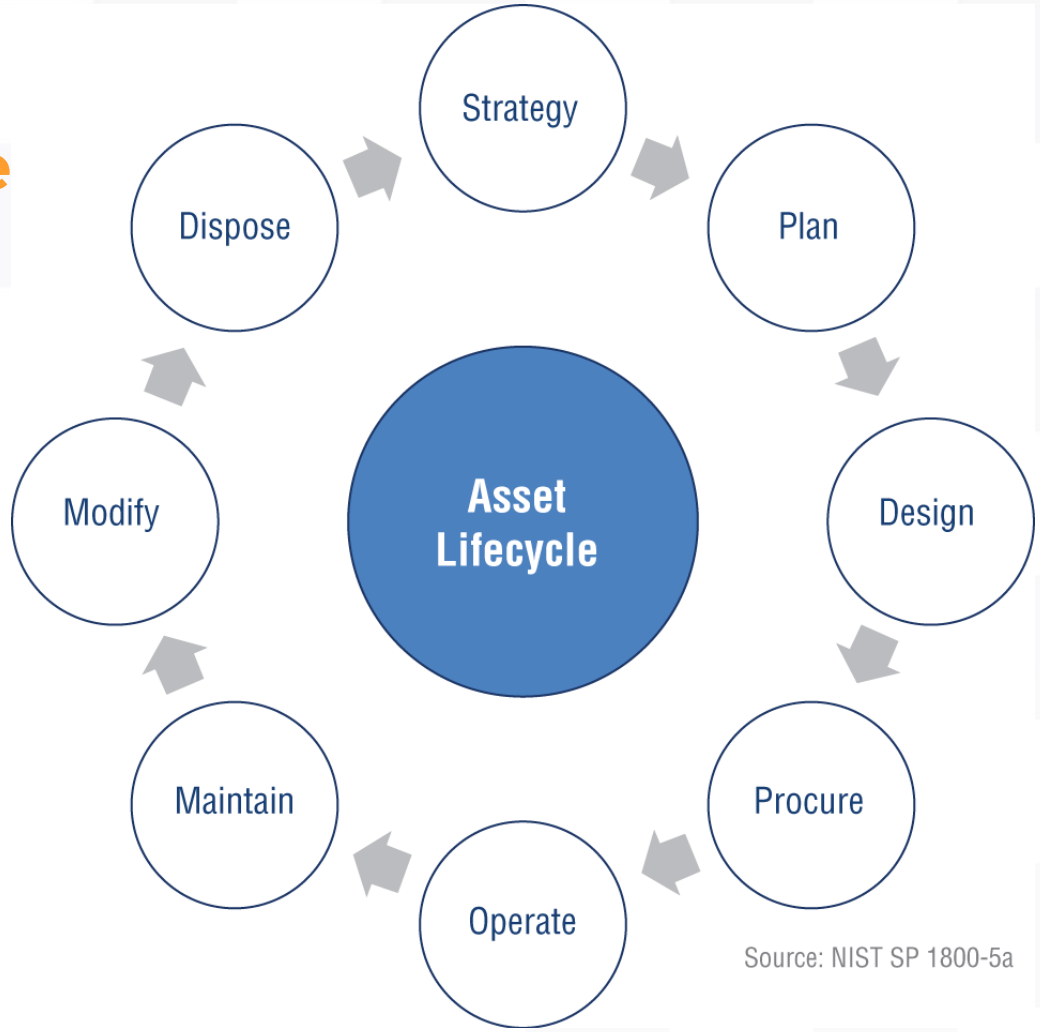
Automate as much as possible!

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

Asset Management

Typical asset management lifecycle
(p. 209)



Questions?
Pls put in YouTube chat or Discord.

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

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

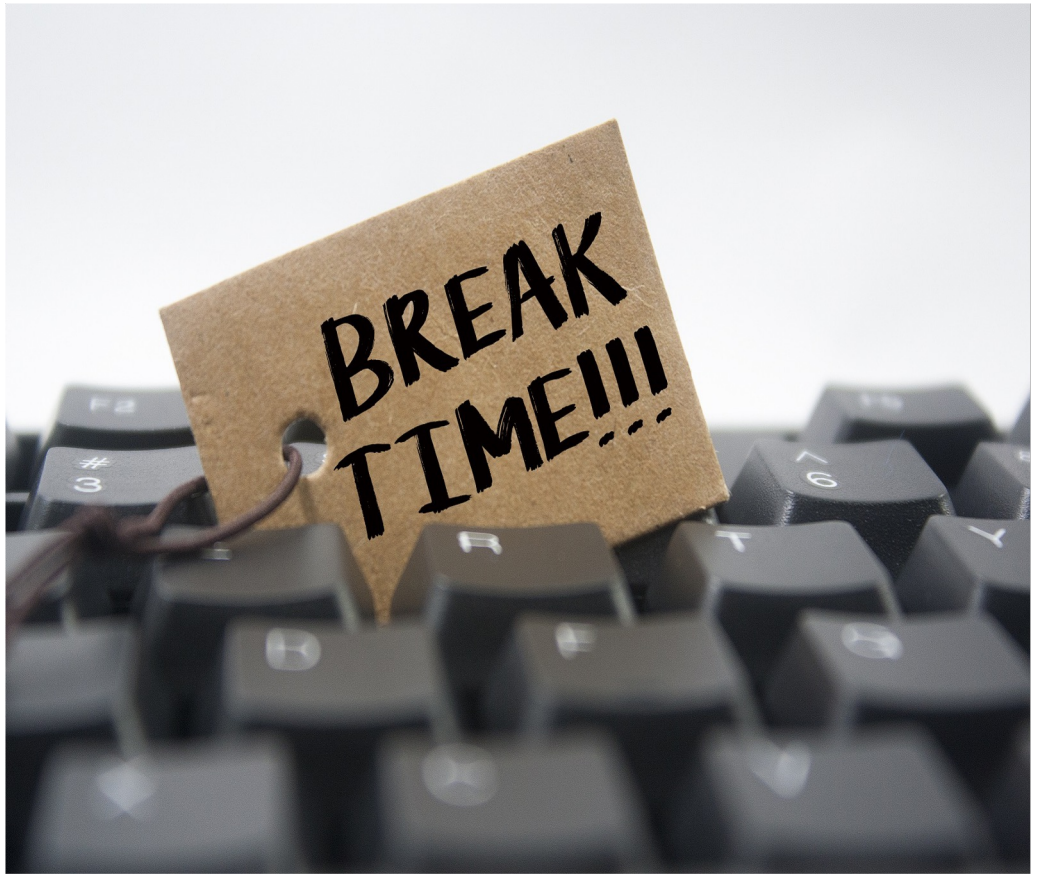
Implementing Asset Management

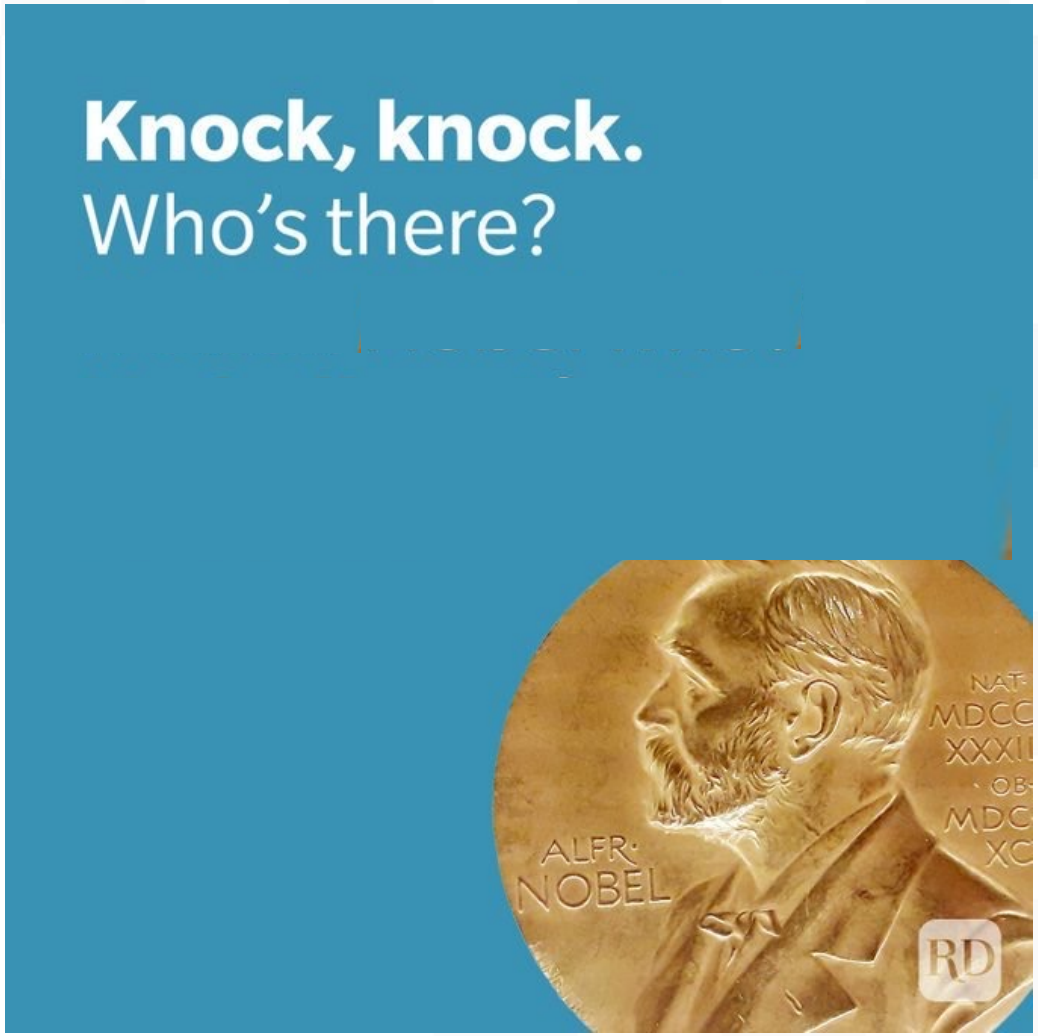
Change Management (p. 213)

- 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 THREE

DOMAIN 2: ASSET SECURITY





CISSP® MENTOR PROGRAM – SESSION THREE

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

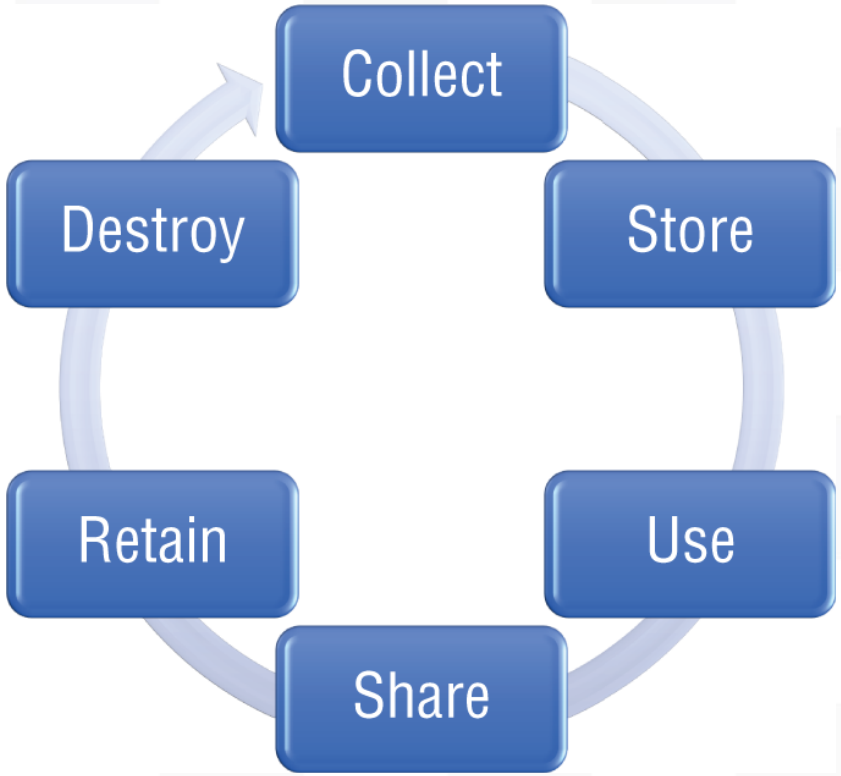


FIGURE 2.5 Secure data lifecycle

DOMAIN 2: ASSET SECURITY

Data Lifecycle (p. 214)

Review

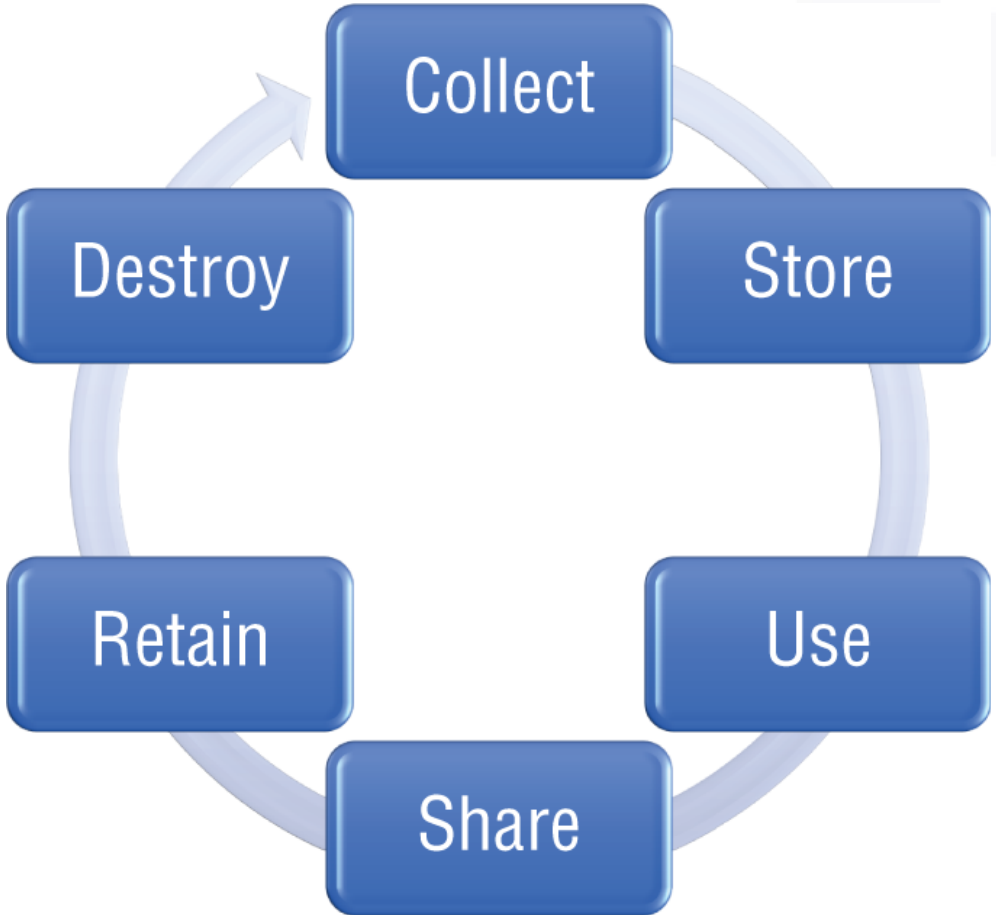


FIGURE 2.5 Secure data lifecycle

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.

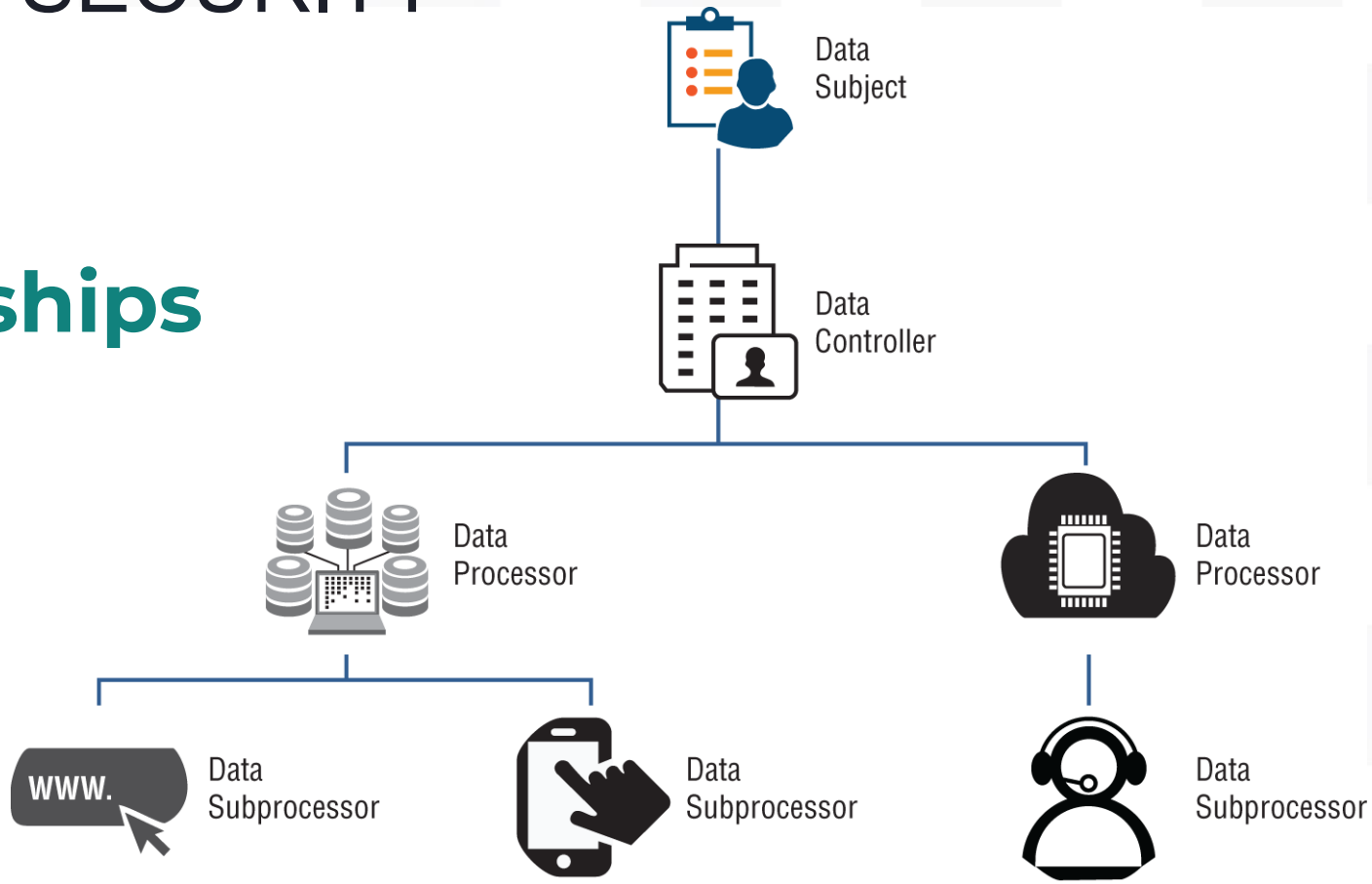
Data Processors (p. 219)

- 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

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.

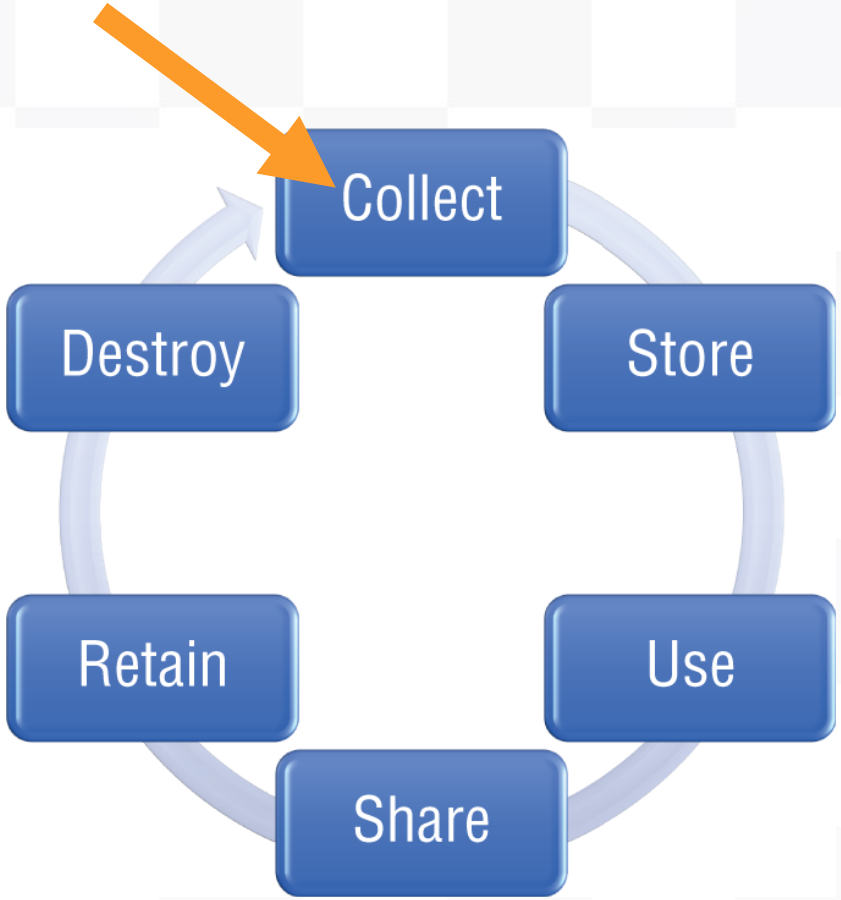
Data Subjects

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

DOMAIN 2: ASSET SECURITY

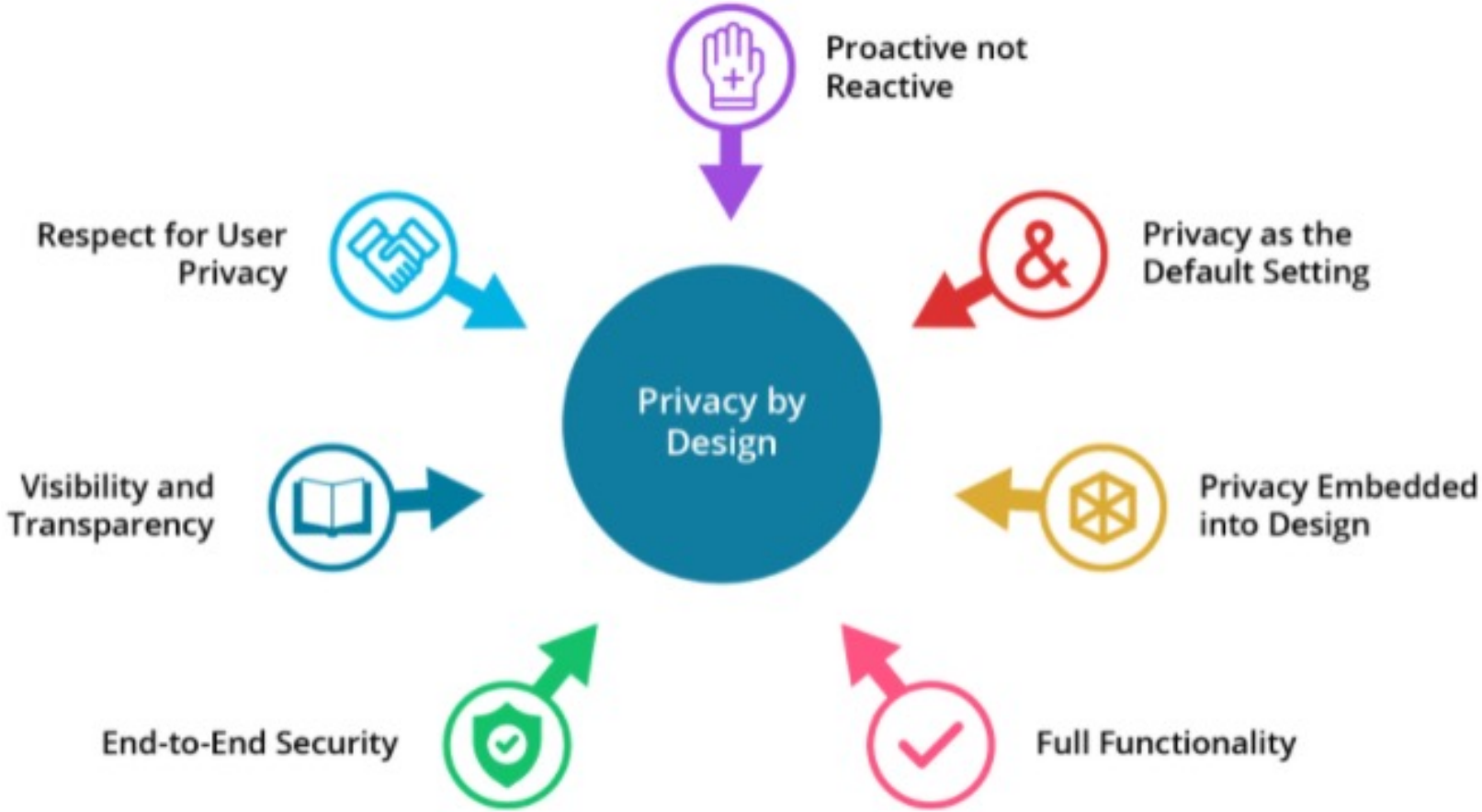
Data Collection (p. 221)

- 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



DOMAIN 2: ASSET SECURITY

Privacy by Design – 7 Foundational Principles



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

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

DOMAIN 2: ASSET SECURITY

Data Management

Privacy Principles

Data Use / Purpose

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

Data Location

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

Questions?
Pls put in YouTube chat or Discord.

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.

DOMAIN 2: ASSET SECURITY

Data Management

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

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.
- d/or formatting a h
  thod for destroying
  on.
- d temporary files (c
  media.

Certificate of Destruction

ISSUE: Cloud Service Providers

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”

DOMAIN 2: ASSET SECURITY

See the 2023 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

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: 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 THREE

DOMAIN 2: ASSET SECURITY

New Topic!

ENSURE ASSET RETENTION (pp. 232-239)

Topics:

- Determining Appropriate Records Retention
- Records Retention Best Practices

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?

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.

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 THREE

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

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.).

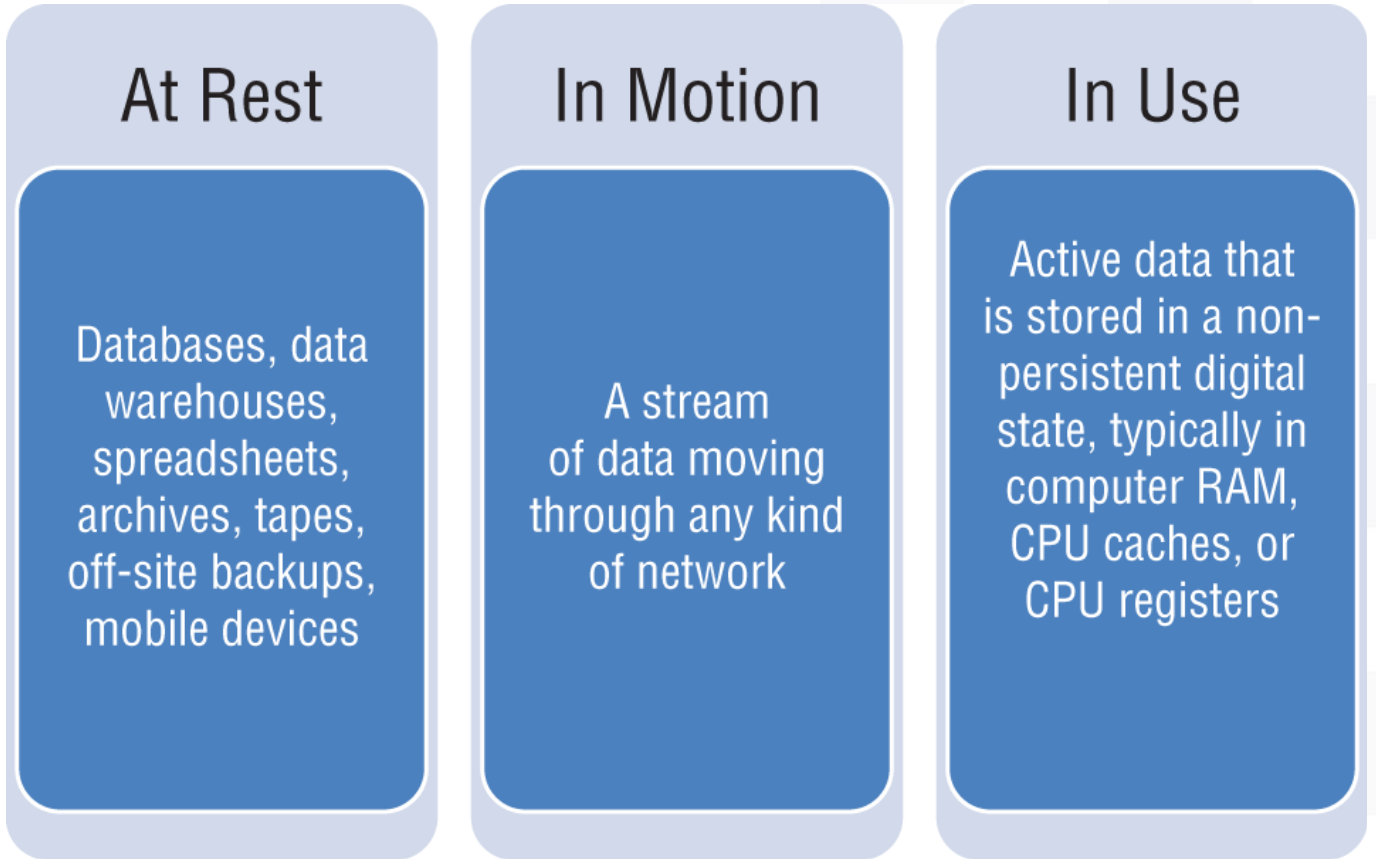
Also discussed Chapter 1

DOMAIN 2: ASSET SECURITY

Data Security Controls

Data States (p. 241-245)

Figure 2.7 Data States and Examples



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

DOMAIN 2: ASSET SECURITY

Covered in Domain 3.

Data Security Controls

Data Protection – *Data in Use*

- 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.

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.”

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)

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 THREE

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.

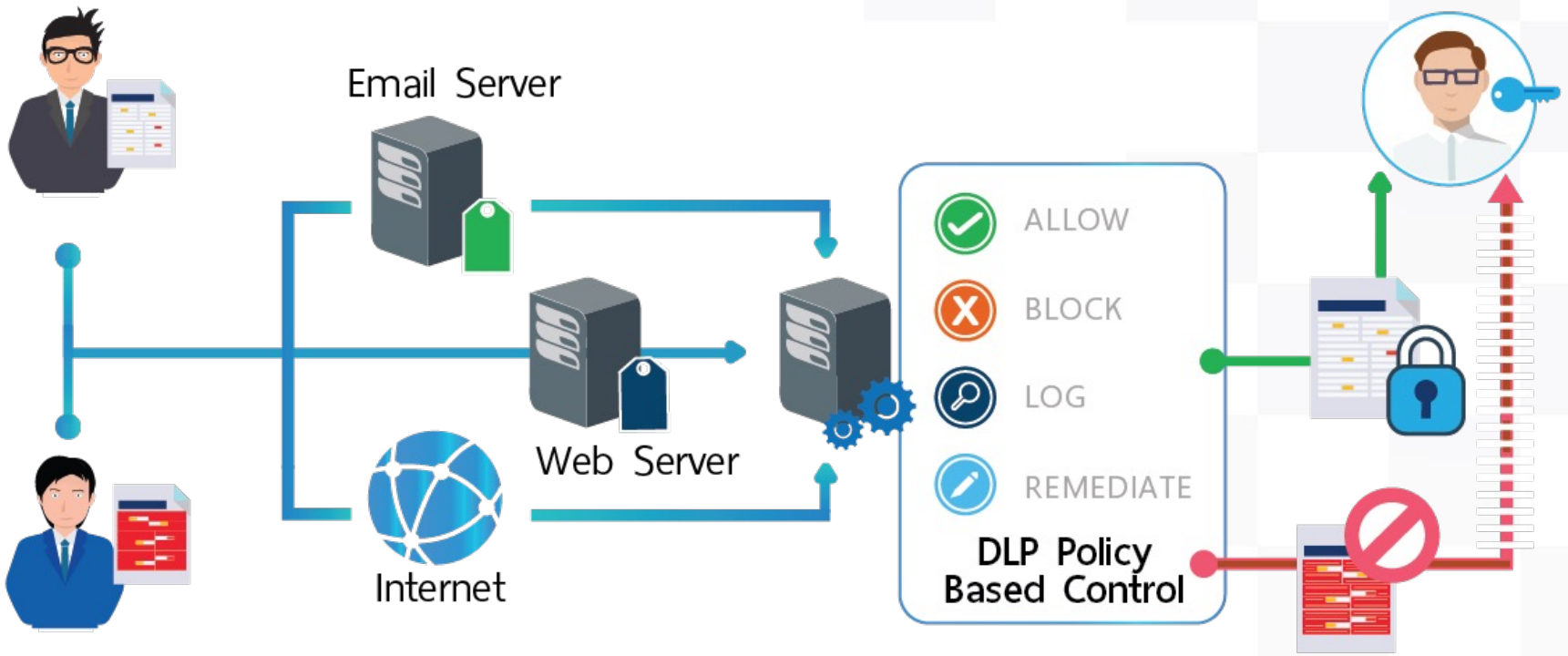
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 2: ASSET SECURITY

Data Protection Methods

Data Loss Prevention (DLP) pp. 255-258

aka Data Leakage Protection



DOMAIN 2: ASSET SECURITY

Data Protection Methods

Data Loss Prevention (DLP) pp. 255-256

3 Core Stages:

1. Discovery & Classification
2. Monitoring
3. Enforcement

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

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

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 THREE

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

DOMAIN 2 - FIN

We made it!

Next Session
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 THREE

INTRODUCTION

Agenda –

- Security Architecture
- Security Engineering
- Security Models
- Security Controls
- Systems overview
- Cryptography

CISSP® MENTOR PROGRAM – SESSION THREE

DAD JOKE

Before we get too deep into this.

How about a dumb dad joke?

I received [illegible] eam pie

HAHAHAHA

Moving on…

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

Security Architecture Is

Design and organization of the components, processes, services, and controls appropriate to reduce the security risks associated with a system to an acceptable level.

Security Engineering Is

Implementation of that design

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

Introduction

- The goal is protecting confidentiality, integrity, and availability of the systems or business in addition to Privacy and other important principals
- Conduct a comprehensive risk assessment to gain an accurate idea of the risks to be addressed.
- Once risks are identified and assessed the security architecture can begin.
- Risk treatments
  - Avoid
  - Transfer or share (i.e., insurance or contract)
  - Mitigate (e.g., through security architecture)
  - Accept

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

Risk assessment

- Initial risk assessment identifies the risks to be reduced through the design of a security architecture to incorporate appropriate security controls.
- An assessment must be made to confirm that the resulting system's risks have been reduced to an acceptable level.
- Cost associated with certain controls can be prohibitive related to anticipated benefit.
- Decision to reduce certain risks may need to be reconsidered, and those risks treated in another manner, avoided through a system redesign, or the project simply abandoned.

*Reminder the **cost of a security control, must be less than the cost of the risk** being addressed

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

Introduction

- Security serves to protect the business. The work of the security architect is to ensure the business and its interests at the very least are protected according to applicable standards and laws, as well as meeting any relevant regulatory compliance needs.
- There is a tendency to concentrate on technical security controls and attempt to address all known security issues or requirements
- Security for security's sake, while intellectually satisfying, is a disservice to the organization.
- Always remember we first serve as subject matter experts, aware of relevant regulations or laws and capable of ensuring our organization's compliance wherever change is required.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

Introduction

- Organization's security strategy must align with its mission, goals, objectives, and compliance environment.

- Success in security architecture is much more likely when one is aligned with the business and taking a risk management approach to security architecture.

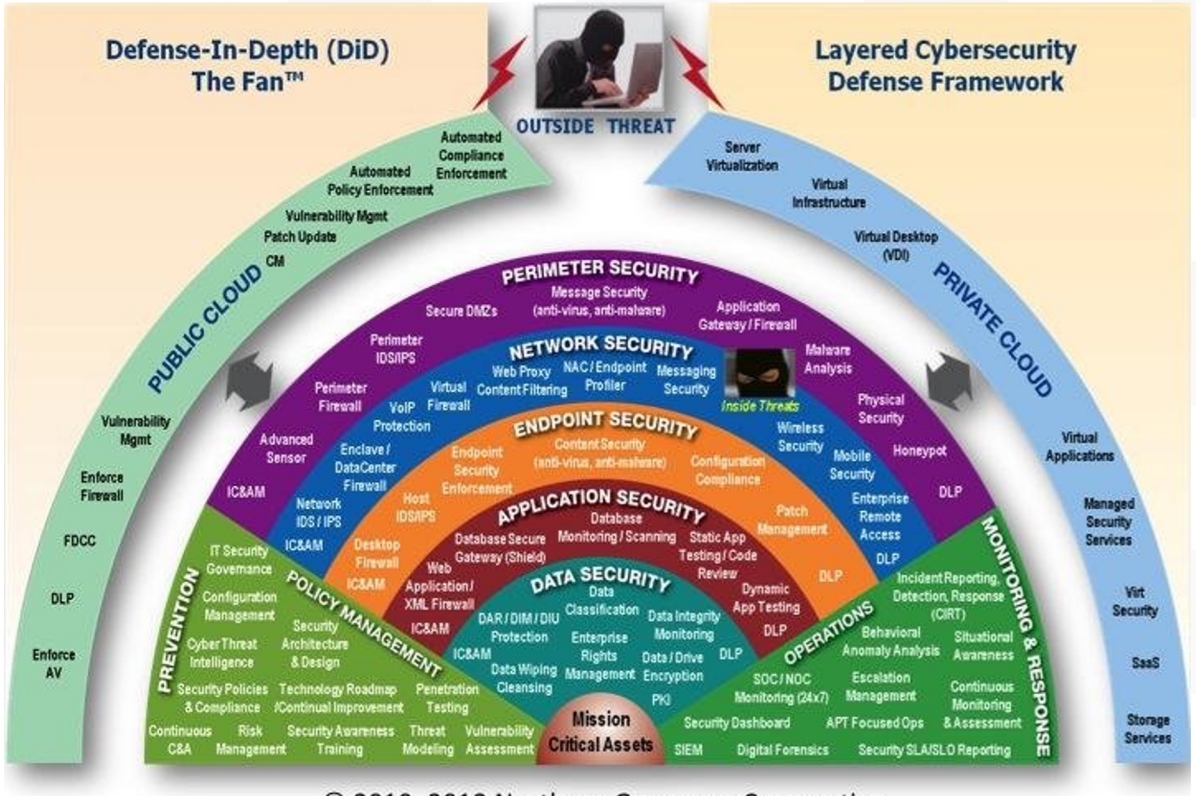
CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

- Design
- Development
- Testing
- Implementation
- Maintenance
- Decommissioning



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

- It is less expensive to incorporate security when the overall functional system design is developed rather than trying to add it on later (which will often require redesign, if not reengineering, of already developed components).
- The need for security controls is not just to prevent the user from performing unauthorized actions, but to prevent components of the system itself from violating security requirements when acting on the user's requests.
- If security is not intrinsic to the overall design, it is not possible to completely mediate all the activities that can compromise security.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

Fundamental to any security architecture, regardless of the design principles employed, are the basic requirements outlined in 1972 by James Anderson in Computer Security Technology Planning Study (USAF):

- Security functions need to be implemented in a manner that prevents their being bypassed, circumvented, or tampered with.
- Security functions need to be invoked whenever necessary to implement the security control. Security functions need to be as small as possible so that defects are more likely to be found.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Domain separation

- Placing components that share similar security attributes, such as privileges and access rights, in a domain.
- Only permitting separate domains to communicate over well-defined and (completely) mediated communication channels (e.g. application programming interfaces, or APIs).

- Real World Examples
  - A network is separated into manageable and logical segments. Network traffic (inter-domain communication) is handled according to policy and routing control, based on the trust level and workflow between segments.
  - Data is separated into domains in the context of classification, categorization, and security baseline. Even though data might come from disparate sources, if that data is classified at the same level, the handling and security of that classification level (domain) is accomplished with like security attributes.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Layering

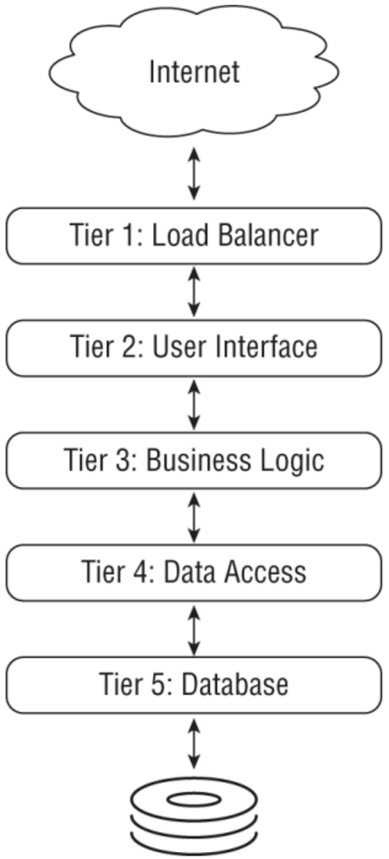
- Hierarchical structuring of a system into different levels of abstraction, with higher levels relying upon services and functions provided by lower levels, and lower levels hiding (or abstracting) details of the underlying implementation from higher levels.
- Layering is seen in network protocols, starting with the classic OSI seven-layer model running from physical through to application layers.
- In software systems, one encounters operating system calls, upon which libraries are built, upon which we build our programs. Within the operating system, higher-level functions (such as filesystem functions) are built upon lower-level functions (such as block disk I/O functions).

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES



DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

The purpose of layering is to do the following:

- Create the ability to impose specific security policies at each layer
- Simplify functionality so that the correctness of its operation is more easily validated

From a security perspective:

- Higher levels always have the same or less privilege than a lower level. If layering to provide security controls, it must not be possible for a higher level to bypass an intermediate level.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Encapsulation

- An architectural concept where objects are accessed only through functions that logically separate functions that are abstracted from their underlying object by inclusion or information hiding within higher level objects.
- Encapsulation functions can define the security policy for that object and mediate all operations on that object.
- Encapsulation requires that all access or manipulation of the encapsulated object must go through the encapsulation functions, and that it is not possible to tamper with the encapsulation of the object or the security attributes (e.g., permissions) of the encapsulation functions.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Encapsulation

- Device drivers can be considered to use a form of encapsulation in which a simpler and consistent interface is provided that hides the details of a particular device.
- Forcing interactions to occur through the abstract object increases the assurance that information flows conform to the expected inputs and outputs.

- An example where encapsulation is used in the real world is the use of the setuid bit. Typically, in Linux or any Unix-based operating system, a file has ownership based on the person who created it, and an application runs based on the person who launched it. A special mechanism, setuid, allows for a file or object to be set with different privileges. Setting the setuid bit on a file will cause it to open with the permission of whatever account you set it to be. The setuid bit controls access, above and beyond the typical operation. That is an example of encapsulation.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Redundancy

- Designing a system with replicated components, operating in parallel, so that the system can continue to operate in spite of errors or excessive load.
- From a security perspective, redundancy is an architectural principle for addressing possible availability and integrity compromises or issues.
- For redundancy to work, it must be possible for the overall system to detect errors in one of the replicated subsystems.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Redundancy examples

- High availability solutions such as a cluster, where one component or system takes over when its active partner becomes inaccessible
- Having storage in redundant array of inexpensive disks (RAID) configurations where the data is made redundant and fault tolerant
- Cloud-based storage, where data is replicated across multiple data centers, zones, or regions

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (5 architectural principles)

Virtualization

- Is a form of emulation in which the functionality of one real or simulated device is emulated on a different one. (This is discussed in more detail in the "Understand Security Capabilities of Information Systems" section later in this chapter.)
- More commonly, virtualization is the provision of an environment that functions like a single dedicated computer environment but supports multiple such environments on the same physical hardware.
- Virtualization involves abstracting the underlying components of hardware or software from the end user.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Security Architecture

RESEARCH, IMPLEMENT, AND MANAGE ENGINEERING PROCESSES USING SECURE DESIGN PRINCIPLES

ISO/IEC 19249 (

- Least privilege
- Attack surface minimization
- Centralized parameter validation
- Centralized general security services
- Preparing for error and exception handling

The principle of least privilege asserts that access to information should only be granted on an as-needed basis

The more entry points, the greater the attack surface.

Full parameter validation is especially important when dealing with user input, or input from systems to which users input data.

Simplifying your security services interface instead of managing multiple interfaces is a sensible benefit.

Systems must ensure that errors are detected, and appropriate action taken

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling

Process to identify security threats and vulnerabilities, and prioritize mitigations

Used to reduce risk and guide secure development.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling STRIDE (6 categories)

- Design
- Development Testing
- Implementation
- Maintenance
- Decommissioning

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling

Process to identify security threats and vulnerabilities, and prioritize mitigations

Used to reduce risk and guide secure development.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling STRIDE (6 categories)

- **Spoofing** Spoofing is an attack during which a person or system assumes the identity of another person or system by falsifying information.
- **Tampering** Data tampering is an attack on the integrity of data by maliciously manipulating data.
- **Repudiation** Repudiation is the ability of a party to deny that they are responsible for performing an action. Repudiation threat occurs when a user claims that they did not perform an action, and there is no evidence to prove otherwise.
- **Information disclosure** Information disclosure — commonly referred to as a data leak — occurs when information is improperly shared with an unauthorized party
- **Denial of service** A denial-of-service (DoS) attack involves a malicious actor rendering a system or service unavailable by legitimate users.
- **Elevation of privilege** Elevation of privilege (or privilege escalation) occurs when an unprivileged application user can upgrade their privileges to those of a privileged user (such as an administrator).

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling STRIDE (6 categories)

- **Spoofing** Spoofing em assumes the identity of another person or system by falsifying information.
- **Tampering** Data tampering is an attack on the integrity of data by malicious
- **Repudiation** Repudiat y are responsible for performing an action. Repudiation threat occurs whe n action, and there is no evidence to prove otherwise.
- **Information disclosure** Information disclosure — commonly referre information is improperly shared with a
- **Denial of service** A denial s actor rendering a system or service unavailable by legitimate users.
- **Elevation of privilege** Elevation of privilege (or privilege esca tion) o user can upgrade their privileges to those of a privileged user (such as an administra

Strong passwords, multifactor authentication, and digital signatures are common controls to protect against spoofing.

Strong access controls and thorough logging and monitoring are good ways to prevent and detect data tampering.

Digital signatures and secure logging and auditing are the primary controls to provide nonrepudiation.

Encryption, data loss prevention (DLP), and strong access controls are common controls to protect against information disclosure.

System redundancy, network filtering, and resource limits are common protections against DoS attacks.

Strong access control and input validation are common protections against privilege escalation.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling STRIDE (6 categories)

- **Spoofing** Spoofing em assumes the identity of another person or system by falsifying information.
- **Tampering** Dat controls and thorough toring are good ways to etect data tampering.
- **Repudiation** R ning an action. Repudiation threat occ dence to prove otherwise.
- **Information d** information is improper ta loss prevention (DLP), ess controls are common tect against information disclosure.
- **Denial of service** A denial s actor rendering a system or service unavailable by legitimate users.
- **Elevation of privilege** Elevation of privilege (or privilege esca tion) o user can upgrade their privileges to those of a privileged user (such as an administra

Strong passwords, multifactor authentication, and digital signatures are common controls to protect against spoofing

QUESTION TO ASK

WHAT CAN GO WRONG??

System redundancy, network filtering, and resource limits are common protections against DoS attacks.

Strong access control and input validation are common protections against privilege escalation.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling DREAD (5 key points)

- **D**amage What is the total amount of damage the threat is capable of causing to your business?
- **R**eproducibility How easily can an attack on the particular threat be replicated?
- **E**xploitability How much effort is required for the threat to be exploited by an attacker?
- **A**ffected users How many people, either inside or outside of your organization, will be affected by the security threat?
- **D**iscoverability How easily can the vulnerability be found?

Uses a numeric value for rating severity of security threats (1-10)

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling DREAD (5 key points)

- **D**amage What is the
- **R**eproducibility
- **E**xploitability Hov
- **A**ffected users
  threat?
- **D**iscoverability

Uses a numeric v

security

D = 4
R = 3
E = 8
A = 5
D = 9
Risk Sum = 29

*There are many opinions on the relative importance of each of the categories within DREAD, and many security professionals disagree with a model that weights each category equally

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling PASTA (7 steps) (Process for Attack Simulation and Threat Analysis)

- **Define objectives** During this first stage, key business objectives are defined, and critical security and compliance requirements are identified.
- **Define technical scope** During this stage, the boundaries of the technical environment and the scope of all technical assets for which threat analysis is needed are defined. In addition to the application boundaries, you must discover and document all infrastructure, application, and software dependencies.
- **Application decomposition** During this stage, an evaluation of all assets (i.e., the application components) needs to be conducted, and the data flows between these assets need to be identified. As part of this process, all application entry points and trust boundaries should be identified and defined. This stage is intended to establish a clear understanding of all data sources, the parties that access those data sources, and all use cases for data access within the application
- **Threat analysis** This stage is intended to identify and analyze threat information from within the system, such as SIEM feeds, web application firewall (WAF) logs, etc., as well as externally available threat intelligence that is related to the system.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling PASTA (7 steps) (Process for Attack Simulation and Threat Analysis)

- **Define objectives** During this first stage, key busine… objectives and compliance requirements are identified.
  - a preliminary business impact analysis (BIA) is conducted to identify potential business impact considerations.
- **Define technical scope** During th… vironment and the scope of all technical assets for which th… application boundaries, you must discover and document all … pendencies.
  - The goal is to capture a high-level but comprehensive view of all servers, hosts, devices, applications, protocols, and data that need to be protected.
- **Application decomposition** During this stage, an evalu… components) needs to be conducted, and the data flows between these a… this process, all application entry points and trust boundaries should be i… intended to establish a clear understanding of all data sources, the partie… use cases for data access within the application.
  - in other words, who should perform what actions on which components of the application.
- **Threat analysis** This stage is… ormation from within the system, such as SIEM feeds, web application fir… available threat intelligence that is related to the system.
  - The output of this stage should include a list of the most likely attack vectors for the given application or system.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling PASTA (7 steps) (Process for Attack Simulation and Threat Analysis)

- Vulnerability analysis During this stage, all vulnerabilities within the application's code should be identified and correlated to the threat-attack scenarios identified in step 4. Operating system, application, network, and database scans should be conducted, and dynamic and static code analysis results should be evaluated to enumerate and score existing vulnerabilities
- Attack enumeration During this stage, attacks that could exploit identified vulnerabilities (from step 5) are modeled and simulated. This helps determine the likelihood and impact of each identified attack vector.
- Risk and impact analysis During this final stage, your business impact analysis (from step 1) should be refined based on all the analysis performed in the previous six steps.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Threat Modeling PASTA (7 steps) (Process for Attack Simulation and Threat Analysis)

- **Vulnerability analysis** D…tion's code should be identified and correlated to the threat…ating system, application, network, and database scans should…ode analysis results should be evaluated to enumerate and s…

The primary output of this stage is a correlated mapping of all threat-attack vectors to existing vulnerabilities and impacted assets.

- **Attack enumeration** During this …s (from step 5) are modeled and simulated. This…ntified attack vector.

After this stage, your organization should have a strong understanding of your application's attack surface (i.e., what bad things could happen to which assets within your application environment).

- **Risk and impact analysis** Du…m step 1) should be refined based on all the analysis performed in the previous six steps.

Risks should be prioritized for remediation, and a risk mitigation strategy should be developed to identify countermeasures for all residual risks.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Secure Defaults (secure-by-default) (SBD)

- The concept of secure defaults (or secure-by-default) essentially means that systems should be designed with the best security possible without users needing to turn on security features or otherwise think about security configurations.
- Secure-by-default means that a system's default configuration includes the most secure settings possible, which may not always be the most highly functioning settings.
- Systems and applications should be designed such that the end user (or system admin) must actively choose to override secure configurations based on the business's needs and risk appetite.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Fail Security

- For some systems, a fail-open design, where systems continue to allow access when exceptions occur, may be preferable to ensure that access to important information remains readily available during a system error or exception. Conversely, a fail-secure (also known as a fail-safe or fail-closed) system blocks access by default, ensuring that security is prioritized over availability.

- For systems with sensitive data, security controls should be designed such that in the absence of specific configuration settings to the contrary, the default is to not permit the action. Access should be based on permission (e.g., allowed list), not exclusion (e.g., blocked list)

- *This is the principle behind “deny all” default firewall rules and also relates to the concept of least privileged

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Fail Security

- If an error is detected, the system fails in a deny (or safe) state of higher security rather than failing in an open, less secure state.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Separation of Duties (SOD)

- Requires two (or more) actions, actors, or components to operate in a coordinated manner to perform a security sensitive operation.

- Breaking up a process into multiple steps performed by different individuals or requiring two individuals to perform a single operation together (known as dual control) forces the malicious insider to collude with multiple insiders to compromise the system.
- More robust and less susceptible to failure

- *Separation of duties can also be viewed as a defense-in-depth control; permission for sensitive operations should not depend on a single condition.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Keep it Simple

- "Complexity is the worst enemy of security. The more complex you make your system, the less secure it's going to be, because you'll have more vulnerabilities and make more mistakes somewhere in the system. … The simpler we can make systems, the more secure they are." – Bruce Schneier

- "If complexity is the worst enemy of security, then simplicity must be its ally" – Evan Francen

- "Simple is securable, complex is chaos waiting to happen" –Ryan Cloutier

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Keep it Simple

- Complexity is the enemy of security. The simpler and smaller the system, the easier it is to design, assess, and test. When the system as a whole cannot be simplified sufficiently, consider partitioning the problem so that the components with the most significant risks are separated and simplified to the extent possible. This is the concept behind a security kernel — a small separate subsystem with the security-critical components that the rest of the system can rely upon.
- By separating security functionality into small, isolated components, the task of carefully reviewing and testing the code for security vulnerabilities can be significantly reduced.

CISSP® MENTOR PROGRAM – SESSION THREE

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

Research, Implement, and Manage Engineering Processes Using Secure Design Principles

Keep

- Complexi … design, assess, and test. Whe … e problem so that the comp … possible. This is the concept b … omponents that the rest of th …
- By separa … eviewing and testing the code …

SESSION 3 - FIN
YOU MADE IT!

Domain 1 and 2 is a done and 3 is ½ done WHOOT HECK YA!! YALL!

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

Homework:

- Read 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 Discord Channel.

See you Wensday!

2022

Class #3 – Domain

Ryan Cloutier

President of SecurityStudio & vCISO
Infosec Missionary on a Mission